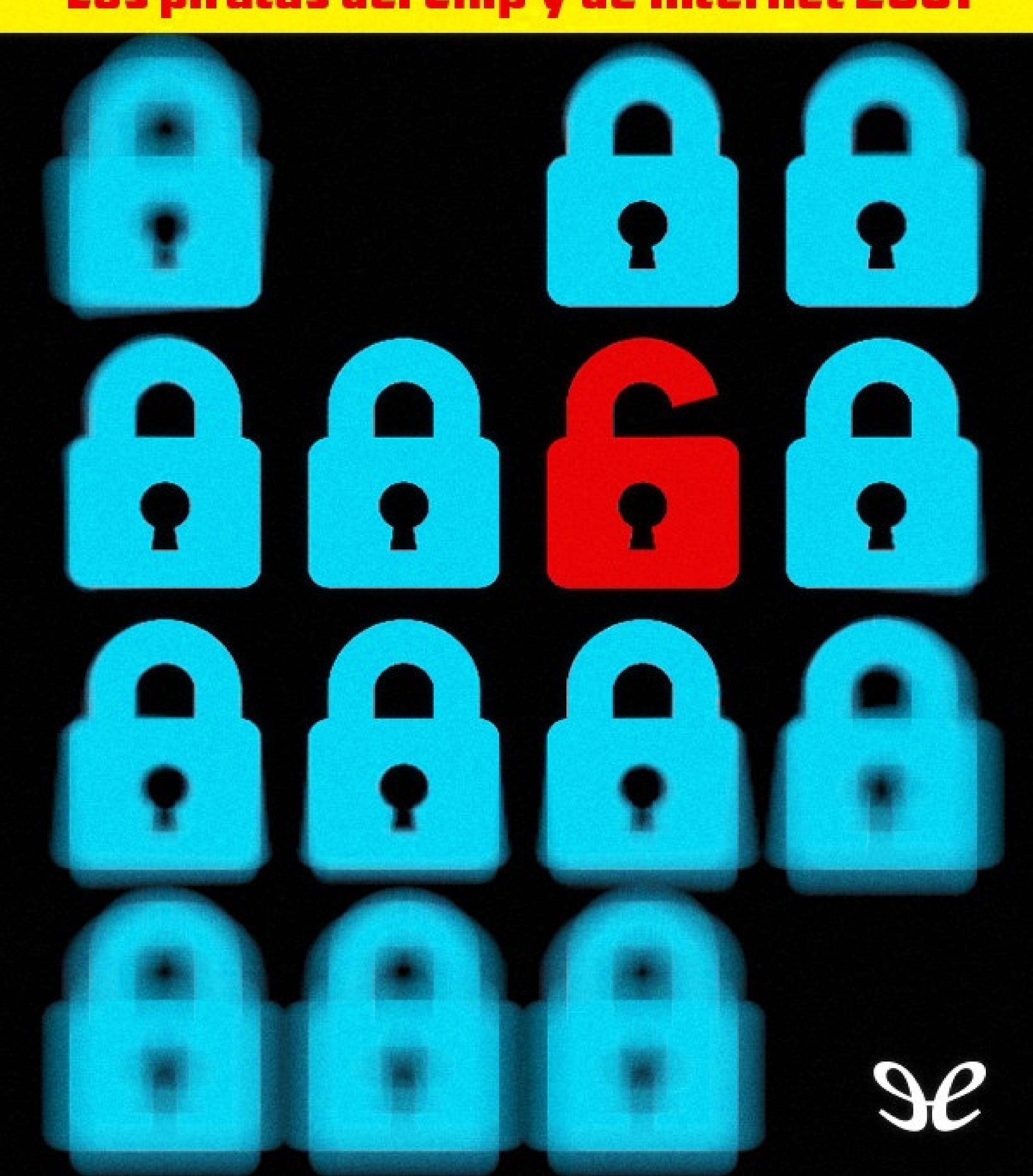
Claudio Hernández

Hackers

Los piratas del Chip y de Internet 2001



Los piratas del Chip y la Internet, de Claudio Hernández, es un libro que gustará a todos aquellos a los que les guste la informática, o tengan curiosidad por conocer como empezó el mundillo de los hackers, los phreakers y los creadores de virus. El libro esta escrito en forma de relatos cortos de casos reales, en su mayoría estadounidenses, pero con un toque literario que hace que su lectura sea bastante amena.



Claudio Hernández

Hackers Los piratas del Chip y de Internet

ePub r1.2
lestrobe 20.10.14

Título original: *Hackers Los piratas del Chip y de Internet*
Claudio Hernández, 2001
Diseño/Retoque de cubierta: mininogris

Editor digital: lestrobe
Erratas: (r1.1) liete
ePub base r1.1



Prólogo

Hakim Bey, el famoso gurú de la red que alcanzó fama -allá por los 70, recuerdo- con el desarrollo de la rebelde teoría TAZ (Zonas Autónomas Temporales) y cuyo auténtico nombre podría ser Peter Lamborn Wilson, escritor, filósofo y poeta que reside, al parecer, en algún lugar cercano a la ciudad de New York, se interrogaba -con motivo del simposio: Incidencias y disidencias. Utopías y antiutopías de la cibercultura, celebrado en la Universidad de Alicante-… Hakim Bey se decía: «he estado esperando años a que los hackers hiciesen algo y ¿dónde están?”

A ún cuando corriera el riesgo -que lo corro- de ser considerado despectivamente un triste lammer -o lamer, según- de los que se asegura no tienen ni p.i. o bien ser tachado de wannabe, siento no coincidir con Hakim, esta vez. Porque los hackers han estado, están y -modestamente pienso- estarán donde deben. Y entre otros, en Internet. Cuestionarse la ubicación intentando tracearlos es inútil. ¿Es así o no, Claudio?

Claudio Hernández - (que se sepa) - no es un hackers, ni un craker, ni tan siquiera un phreaker. Con el máximo respeto a todos debo anunciar que Claudio es, también, otro auténtico experto que viene a unirse al mundo informático. Y, para mi, todo un descubrimiento de última hora. Yo no le he conocido a través de ningún agujero, bug u hole que se precie. Tampoco he usado de backdoor alguna que pudiera servirme en un exploit. Ni ataques asincrónicos, ni las llamadas bombas lógicas. A él hay que entenderle por sus textos. Sus extraordinarios, complejos y científicos textos. Los libros que Claudio escribe no tienen firewall que impida el acceso a su comprensión, muy al contrario. Leerle no es hacer ingeniería social, ni se precisa conocer PPP, TCP/IP o UDP. Para recepcionarse en sus páginas no se hace necesario login protocolario alguno, ni asumir el rol del pirata informático. Que no. Si se me permite la expresión, aseguraría que Claudio Hernández es, tal vez, un sysop del conocimiento informático a la par que un root literario que describe a los personajes con acierto.

Kevin Mitcnick, por ejemplo, es una de esas figuras legendarias que tan inteligentemente están explicitas en los textos de Claudio Hernández. Con minuciosidad, paso a paso, sin necesidad de usar superzapping, sin tener que sacar password alguna de entre las lineas ortográficas, Claudio nos narra, nos hace como un criptoanálisis del verbo en si. En un alarde de paciente conocimiento nos va adentrando en esa pedagogía de altura casi sin darnos cuenta. Cuando lo adviertes ya estás participando de su ciencia ávidamente. Página a página. Es difícil comenzar un texto de Claudio Hernández y no leérselo de un tirón. Te entusiasma, se queda en tu mente como un caballo de troya cualquiera que hubiese madrugado para hacer trashing electrónico en tu cerebro físico. Y te cuesta olvidarle porque sus obras son

magistrales.

Recomendar el libro de Claudio Hernández no es ninguna obligación, es un placer. Como pedagogo puedo aseverar con rotundidad que se aprende mucho prestando la debida atención a su contenido. Y quién sabe si, saturados de su ciencia, algún día podamos llegar a navegar por ese lado oscuro de la red y curiosamente olisquear… sin causar daño a nadie ni a nada. Porque hay que ser tan respetuosos con los demás como con uno mismo. Que quede suficientemente claro. Y a nadie le apetece ser crackeado, aparte -es obvio- de lo delictivo que supone esa tarea ilegal. Quiero terminar diciendo, como al principio, que Claudio Hernández no es ningún hackers, (ni yo tampoco) aunque… ¿Tu qué piensas de ello, querido lector?

Sinceramente creo que ha llegado el momento de marcarme un logout, lo más rápidamente posible. Pero antes del adiós informar que el libro de Claudio Hernández, por gentileza del autor, se encuentra disponible gratuitamente (entre otros lugares) en mi página web cuya url figura al pie. Hasta siempre…

Profesor J. Jesús Parras
e-mail: jparras@inforvip.es
Webmaster de La Casa de Jara
http://www.lacasadejara.org

Introducción

Últimamente, escribir un libro sobre Hackers se ha convertido en una labor de «clasificación» de contenidos y datos. Digo esto porque, es obvio que encontrará, a lo largo de la bibliografía sobre Hackers, libros escritos que enseñan el arte de Hackear sistemas y libros en los que se basan en historias de Hackers. El orden no es necesariamente este. Al principio, solo unos cuantos escritores como John Markoff, Steven Levi o Paul Mungo entre otros, se aventuraban a revelar algunos aspectos del Hacking. En realidad, lo que hacían, era relatar las hazañas de los Hackers. Por esta razón, solo podías saber que cosas eran capaces de hacer, pero no como se podían hacer.

Eran tiempos de relatos y de historias de Hackers, pero era un buen comienzo. A día de hoy ya es posible encontrar otro tipo de libros en los cuales te enseñan con pelos y señales las tácticas y técnicas de los Hackers. Son los nuevos escritores, en realidad Hackers convertidos a escritores, que con la escusa de escribir un manual técnico para el Administrador de Redes, revelan las técnicas mas preciadas por los Hackers. Este es el segundo paso, lo que significa que en parte, el miedo ha pasado a un segundo plano. Ahora el miedo se convierte en poder. El libro que más técnicas recopile, es el mejor. Fuera, están esperando toda una tribu de principiantes de Hacker, que patalean si no les cuentas todo. Es posible que a estos personajes les importe poco las hazañas de los demás, ellos solo quieren poner en practica las técnicas de los Hackers, y convertirse algún día, en Hackers respetados.

Sin embargo me pregunto a mi mismo, acaso no interesan las «batallitas» de los demás?. Acaso un libro que solo recopile anécdotas o historias, no es un libro realmente bueno?. Mi experiencia propia me ha demostrado dos cosas. Primero, que un libro que narra las aventuras de unos cuantos Hackers es bien aceptado dentro y fuera de los movimientos Underground. Segundo, que los libros que revelan técnicas son los mas perseguidos por esta misma comunidad, ya que están ansiosos por aprender y devorar todas las combinaciones de teclas posibles. Estas conclusiones, me han llevado a la decisión de escribir un libro como este, el que tienen entre sus manos. Un libro que mezclara de forma hábil, historias y aspectos técnicos del Hacking. Una combinación explosiva, que permitirá mantener el interés de toda la comunidad Underground y que así se espera. Así, en este libro encontrara relatados algunas batallitas de Hackers, lo que le servirá de fuente de inspiración, al tiempo que encontrara capítulos que traten sobre temas más específicos como la criptografía, los Virus informáticos o el Cracking. En definitiva, este es, un libro estudiado y escrito para abarcar a un mayor numero de lectores posible, desde el interesado por las nuevas tecnologías, el que quiere conocer algo mas acerca de esta explosión informática y el avezado que quiere ser Hacker de mayor.

La necesidad de escribir un libro como este era evidente. La actividad del Hacking fuera del ordenador y de la red de Internet, a cobrado fuerza y es quizás aun más peligrosa que tal como la conocemos a través de los medios de información. Sin embargo, voy a abordar en este libro todos los grados del hacktivismo, dentro y fuera del ordenador personal, dentro y fuera del espionaje industrial y en definitiva en todos sus aspectos más conocidos y los menos conocidos. Así, la clandestinidad impera por todas partes, pero no es ese el tono que elegiré en el presente libro.

El Hacking es una realidad y quiero exponer sus fundamentos. Escrito desde España, el libro quiere demostrar como el Hacking también ha hecho furor en nuestro País. Al contrario de lo que se creía, en nuestro país, el grado de piratería es superior al resto de los países de todo el mundo. Sin embargo hay que saber diferenciar lo que es la piratería y lo que es el verdadero rol del Hacking.

Cualquiera de nosotros, cuando intentamos copiar una película de video, esta atentando con la piratería. Eso no es un Hacking. Si no un grado de clandestinidad y un acto de violación de los derechos de autor. El Hacking rivalida este hecho con otra intromisión. El Hacking simplemente nació como un estado de diversión y satisfacción personal y durante muchos años a revestido diversos significados. Obviamente todos los comentarios acerca del Hacking han resultado siempre acusadores y negativos. Pero la culpa no esta en el hecho de hacer Hacking, sino en el uso que se hace de él.

Hacker es una palabra prácticamente intraducible que ha revestido, a lo largo de los años, diversos significados como ya se ha dicho. Pero parece ser que este acrónimo se vincula muy especialmente a los llamados Hacks o dicho de otra manera, así se llaman los golpes secos que efectuaban los técnicos de telefonía cuando intentaban reparar alguno de sus aparatos. Estos golpes secos recibían el nombre de «hachazos» o en elargot ingles Hacks y es mas que probable que quiénes lo hacían se denominaban Hackers. De cualquier forma nunca sabremos con certeza el origen de esta palabra, pero eso hoy por hoy prácticamente da igual, ya que la mayoría de nosotros sabemos que es un Hacker según se nos muestran en los medios de comunicación.

Lo que no se nos ha dicho sobre el Hacking, es quienes son en realidad y que hacen. A menudo leer sorprendentes fechorías o trastadas que un grupo de chicos tímidos de gafas gruesas han hecho a tal o cual ordenador, es a su vez una vaga forma de camuflar el verdadero Hacking. Sin embargo hay que reconocer que eso también es Hacking, pero permítame que le diga que estamos entrando en otros terrenos que van mas allá de la especulación y el saber. Si bien es un grado de clandestinidad o delito introducirse en otro ordenador remoto, lo es también hacer una fotocopia en cualquiera de las páginas de este libro. De cualquier forma ante unas leyes nacidas por el bien de unos pocos, la mayoría de nosotros somos unos verdaderos

delincuentes.

Pero quiero dejar bien claro el tratamiento que se le puede dar a este pequeño grupo de «sabios» antes de continuar explorando los inicios de esta nueva generación. Un Hacker es una persona, sin importancia de edad con amplios conocimientos informáticos o electrónicos que a su vez descubre la intolerancia de algunos organismos por proteger ciertas cosas o intereses. Un Hacker no solo habita en los suburbios de una gran red como lo es Internet, ni navega continuamente entre los discos duros de los ordenadores, que aunque se les conocen en estos entornos mayoritariamente, los Hackers también fisgonean sistemas fuera de una CPU. Solo tenemos que echar una ojeada a nuestro alrededor para saber cuantas cosas mas atentan contra la curiosidad.

Hacer una llamada de teléfono supone un reto muy importante para alguien que no tiene dinero, pero no es esa la intención. Sin embargo si lo que se desea es conocer bien los sistemas de conmutación de una red de telefonía inteligente, que mejor que dejarse atrapar por ella para beber de sus consecuencias. Ya en la segunda Guerra mundial se cifraban los mensajes y las comunicaciones y hoy por hoy todas las comunicaciones de los Satélites están encriptadas. Llegados a este punto un Hacker descubre que todo es una farsa y una gran manta secreta que lo oculta todo. El mundo esta lleno de misterios y de demasiados secretismos.

Sin embargo la gula se lo come todo. El hambre no se sacia y se culmina con una proeza delictiva. Violar los secretos de una comunicación convierten a uno en un Cracker, algo más devastador que un simple fisgoneo de Hacker. Como una extensión mas, surge el Carding, otro fenómeno capaz de clonar las tarjetas de crédito bancarias ytarjetas de acceso inteligentes de canales de pago. Después se crean los Warez, programas informáticos duplicados para sobrevivir en este devastador mundo de la información.

Solo en España el uso fraudulento de estos conocimientos ha conocido un ascenso espectacular. Y en Estados Unidos el pasado año se dejaron de percibir mas de 63 000 millones de pesetas por estos conceptos. Por otro lado se estima que cada día nacen o se crean entre tres y cuatro nuevos virus informáticos y uno de cada dos estudiantes de informática entra en el ordenador de su compañero robándole el password. Todo esto es lamentable, porque la tendencia a desaprovechar las energías positivas va en aumento.

Un buen conocimiento debe ser empleado para mejorar los sistemas en los que se trabaja, pero es más fácil hincharse de satisfacción con un rictus en los labios demostrando que acabas de joder un ordenador o un teléfono.

Estas son las decisiones mal intencionadas y las que más perjudican al verdadero Hacker. Una imagen borrosa sobre este personaje puede echar por la borda todo el buen saber de estas «entes». Otro caso negro para el Hacking son los 15 000 millones

de pesetas que se dejaron de percibir en Europa por el uso fraudulento de tarjetas de acceso inteligentes clonadas de los canales de televisión de pago Europeas. Un Buen Hacker no habría puesto en circulación estas tarjetas, pero si hubiera enseñado a los demás, dentro de su pequeño foro disciplinario, como funcionan este tipo de tarjetas por el mero hecho de decir lo se todo sobre ella y creo que posee un fallo…

Un bug, una codificación mediocre, son las fuentes de interés para un Hacker para mejorarlo. Una complejidad en los mecanismos de seguridad de cualquier sistema informático o electrónico despiertan en él un interés creativo. Después toma notas, las notifica y alguien hace mal uso de ellas.

Es el lado oscuro del Hacking.

Nadie es de fiar allí dentro ”me refiero a Internet» y fuera se dan los conocimientos que se quieren por un puñado de periodistas inexpertos en el tema. Después todo hace explosión en un cóctel sin sabor y todo el mundo te señala como alguien realmente perverso e irónico.

Pero hay que tener en cuenta ciertas cosas interesantes para mejorar la seguridad de los sistemas de nuestro complejo mundo. Un sistema de seguridad de por sí no tiene mucha consistencia si no es atacado por alguien de fuera. En este proceso se demuestra la fuerza del sistema. Si el intruso entra es porque existe un error en el diseño. Así, si no es por el intruso los creadores del sistema de seguridad nunca sabrían que existe un agujeronegro en su sistema. Después el intruso es sometido a un estudio y se le pide colaboración ya que normalmente siempre tendrá mas conocimientos que el propio creador y esto es porque se preocupa realmente de la seguridad del sistema. Es un reto demostrar todo lo contrario y lo consigue.

Y al contrario de lo que se pretendía, no se castiga al intruso, sino que se le contrata en la gran empresa. Esta es la política que persigue un buen Hacker. Sin embargo buenos, lo que se dicen buenos los hay bien pocos.

El mal uso de los conocimientos y el poder casi infinito que uno puede tener con ellos, en un mundo dominado por el conocimiento y la tecnología, ponen en tela de juicio cualquier intento de Hacking. Ya que hoy por hoy cualquier modificación en un fichero informático o una conmutación en un descodificador de señales de televisión, es un acto de consistente violación de los derechos de copyright. Por ello la dominación de la tecnología es absoluta.

Hasta aquí he replanteado la posibilidad de que no todo el Hacking es malo y de que no solo los Hackers habitan en los ordenadores. Aunque es cierto que los ordenadores han popularizado enormemente a los hackers en los últimos años, no es cierto que solo habitan en ese submundo, ni tampoco es cierto que se emplean bien los conocimientos con fines científicos y no lucrativos. Por desgracia el hacking se ha convertido en el índice de un gran libro de insolencias e intromisiones peligrosas. Por lo que definir correctamente el Hacking se hace especialmente complicado.

Que aunque existen desde hace muchísimo tiempo, es ahora cuando conocen su propio acrónimo en el argot técnico y es ahora cuando la tecnología brinda la oportunidad de serlo con mas fuerza, ya que hay que reconocer que la proliferación de ordenadores personales, la red de Internet y los miles de comunicaciones encriptadas, son un gran caramelo sin saborear. Las tecnologías evolucionan y con ella los Hackers se ven forzados al limite de sus actuaciones. Fisgonear un ordenador o tratar de descodificar un canal de pago es siempre un acto delictivo, por lo que por mucho que hablemos, siempre estaremos catalogados como delincuentes informáticos y tratar de quitarse esa mascara es tarea imposible.

Hoy por hoy todo cuanto se crea, reposa sobre la base de los códigos y las encriptaciones para sacar el mayor rendimiento de la tecnología y el producto.

Los programas de ordenadores son un buen ejemplo de ello. Las televisiones se han convertido en canales de pago temáticas y a la carta que requieren de sistemas complejos de encriptación y control para asegurarse una rentabilidad del canal. Losnuevos soportes de grabación ya son digitales para todos los sistemas ya sean de vídeo, audio o datos y poseen códigos de protección contra copias piratas. A su vez todos estos soportes digitales, tales como un simple CD, DVD o Minidisc pueden estar encriptados y reducidos a un puñado de códigos que hacen de ellos una forma de pago por visión.

Esto es, pagas y ves.

Ante este panorama se hace obvio que siempre habrá cierta curiosidad por «estudiar» estos códigos y estas propias tecnologías. Vivimos en un mundo de códigos, encriptaciones y rupturas de sistemas. Sin embargo como creo haber dicho ya, este fenómeno se remonta mucho tiempo atrás, desde que se emplearan las palomas como mensajeras. En cierta época los mensajes eran cifrados y convertidos a un puñado de palabras indescifrables y ya existían quienes descifraban el mensaje del enemigo. Por aquel entonces no se conocían como Hackers y ni tan siquiera estaban penalizados. Solo la llegada del ordenador ha revolucionado este sector y solo desde los ordenadores se ha hablado mucho sobre los Hackers.

Desde aquí queda poco más que contar. Podría estar contando batallitas de Hackers hasta perder el pulso de la pluma, sin embargo creo que eso seria oportuno para otra ocasión. En esta introducción me conformo con definir por encima lo que es un Hacker y especular superficialmente sobre ellos. Defenderlos o acusarlos seria caer en un grave error. Según por donde se mire sé actuaría de una u otra forma.

Criticar los hechos podría ser nefasto y entraríamos en denuncias continuas que no son precisamente la ideología de este libro. Defenderlos hasta la muerte podría ser también otro error, ya que podríamos pecar de egocentrismo. De modo que solo queda exponer los hechos, o mejor dicho de otra manera, solo queda opinar y exponer mis criterios. Sentar las bases de lo que es el Hacking y explicar o mostrar los

conocimientos adquiridos en un terreno complejo y difícil como es el mundo de las nuevas tecnologías, tecnología que agrupa la informática, las comunicaciones y los sistemas de pago por televisión.

Si, ha leído bien, los sistemas de pago por televisión también son el objetivo de la mayoría de los Hackers, de sobras es sabido de la existencia de Software para descodificar canales de pago. La criptografía también está presente en esta área de las nuevas tecnologías y los nuevos Hackers se especializan, cada vez mas, en el tratamiento de algoritmos y sistemas de cifrado, que tan empleados están siendo en la televisión y en la informática. Este es, en definitiva, el mensaje que quiero haceros llegar.

Ahora solo me queda decirles, que espero que disfruten con esta obra, y que aprendan tanto como yo aprendí al escribirla.

Claudio Hernández

Aguilas Noviembre 2000 - Junio de 2001

Capítulo 1 La historia de la Tecnología de hoy

Cada vez que escribo sobre la existencia de los Hackers, siempre surge la misma pregunta del millón. ¿Quién fue primero?, o al menos, cuando se inició la era del Hacker. Siempre empiezo explicando que el termino Hacker se acuñó cuando un técnico de telefonía asestaba un golpe seco al aparato de teléfono para arreglarlo, algo que habitualmente funcionaba.

Esto significa, que de ser cierto, que lo es, el termino Hacker nació en un momento en el que las computadoras eran grandes armatostes como las habitaciones de una casa victoriana. En su interior, cientos de cables se caldeaban al lado de las válvulas de vacío, lámparas mágicas se apresuraban a decir los técnicos.

Eran tiempos del Eniac, de la TX-0 o del MIT. Pero si esto es cierto, los Hackers surgieron en esa época. O quizás surgieron cuando un conocido escritor de novelas de ciencia-ficción los reflejaba en una de sus obras y ya sabéis de quien hablo. En nuestro país, el termino Hacker nació, cuando este que escribe, se decidió a coger la pluma y plasmarlos en unas amarillentas paginas.

Entonces corría el año 1990 y la televisión de pago había sido Crackeada, Internet ya existía para unos cuantos y en el kiosco apenas podías encontrar una o dos revistas de informática. ¿O eso fue después?. En cualquier caso, el principio fue eso, solo el principio de una larga historia.

1.2. Los primeros Hackers

Quien dice primero, puede estar mintiendo, pero también es cierto que parece que todos apuntan a que fueron los chicos de MIT, los primeros en acuñarse la denominación Hacker. Estos eran un grupo de alumnos del prestigioso y conocido Massachusetts Institute of Technology (MIT), en su mayoría miembros del Tech Model Railroad Club (TMRC, Club de Modelos de Trenes) que en 1959 se apuntaron al primer curso de programación que la institución ofreció a sus alumnos, y que se enamoraron de los ordenadores y de lo que se podía hacer con ellos. Esta bella historia de amor «tecnológica» precipitó que los chicos pensaran de otra manera con respecto a la forma de funcionar con los ordenadores de aquellos días.

Estos ordenadores eran unos aparatos demasiado carísimos y más que

descomunales que, con un poco de suerte, ocupaban salas enteras que rápidamente impregnaban con un olor a chamuscado el ambiente de la sala. Para contrarrestar esto, los enormes ordenadores necesitaban complejos sistemas de aire acondicionado que los ventilaran continuamente.

Ademas, estos gigantes de la informática necesitaban de una gran carga de suministro eléctrico para funcionar y subsistir, por lo que el acceso a éstos estaba realmente restringido para los estudiantes, lo que desembocaba en que en pocas ocasiones era el usuario final el que manejaba el ordenador directamente, sino que habitualmente se veía obligado a dar sus programas a los operadores, que a su vez se encargaban de introducirlos en el ordenador y de devolverle los resultados después.

Evidentemente, esto a los chicos del TMRC esto no les bastaba, y aparte de ingeniárselas para que en ocasiones les dejaran introducir directamente programas a ellos mismos y para tener tanto contacto como les fuera posible con el ordenador, no les suponía ningún problema el usarlo desde una sala de terminales a la que en realidad no tenían acceso de modo oficial colándose en ella por las noches. Lo que realmente les importaba a estos chicos, era poder usar el ordenador, sin preocuparse de las menudencias administrativas que dictaban una forma «oficial» de acceder a él.

Poco tiempo después de aquel curso llegó al MIT el TX-0, un ordenador revolucionario para la época, y el grupo de pirados de la informática del MIT tuvo la suerte de que Jack Dennis, un antiguo miembro del TMRC y ahora profesor del MIT, les diera acceso prácticamente ilimitado a esa máquina. Para ellos, una de las principales ventajas que tenía ésta era que en lugar de interactuar con los usuarios mediante tarjetas perforadas, tenía un teclado gracias al cual era posible trabajar directamente con él, lo que les permitía ver directamente el resultado de su trabajo, con lo que cada vez empezaron a pasar más y más tiempo con el ordenador y pronto eran capaces de hacer cosas con él que ni sus diseñadores hubieran creído posibles.

Fue en éste entorno y en ese momento cuando el término hacker se empezó a aplicar a aquellos pirados de la informática capaces de hacer maravillas con un ordenador.

En cualquier caso, la contribución más importante de este grupo de hackers a la historia de la informática no fue la de adoptar ese término sino la de ser los primeros en pensar diferente acerca de cómo se usaban los ordenadores y de lo que se podía hacer con ellos, y, sobre todo, la creación de una ética que regía su comportamiento que aún sigue vigente hoy en día y que todos los hackers siguen (o dicen seguir) en mayor o menor medida, sobre todo en la parte que mantiene que la información debe ser libre.

Esta historia, ha sido repetida una y otra vez, en la mayoría de los reportajes que se han escrito sobre Hackers, ya que de alguna manera se describe con certeza a los primeros Hackers o al menos, cuando se acuño este termino. Por mi parte creo que

podría ser un gran acierto, pero es evidente que no toda la historia del Hacktivismo se ha escrito todavía aun a día de hoy. Por esta misma razón decidí que este era el texto que se iba a publicar, cuando «Bicho» me paso un borrador de un articulo sobre Hackers, empujado por Álvaro, un gran amigo mío, que me pidió que interviniera en el proceso del reportaje.

La descripción de las hazañas de los «locos por los ordenadores» del MIT estaba bien narrada y ademas aporta un dato importante a la historia del Hacktivismo, sin embargo hay quien opina que el Hacktivismo comenzó después, ya que el Hacktivismo parece tener una relación directa con el Phreaking, en un momento en el que reinaba la Bell Telephone.

Este comienzo está bien descrito en el libro *The Hacker Crackdow* de Bruce Sterling, al que llama la Caza de Hackers. Entre 1960 y 1969 tuvieron algunos de los hechos más destacados en el mundo del teléfono. Dos de los artífices de estos hechos son Dennis Ritchie y Ken Thompson que curiosamente no aparecen en el libro de Sterling. Ambos, denominados dmr y Ken, crearon sus fuerzas con el legendario laboratorio de Bell. Eran unos técnicos muy cualificados, lo que en 1969 les llevo a crear importantes aplicaciones para UNIX, un elegante sistema operativo para mini computadoras, ya que así se les llamaba a los ordenadores.

Sus hazañas con los teléfonos de Bell nunca fueron publicadas, por lo que al igual que Bill Gates, se les recuerda como unos jóvenes Hackers que hicieron algo interesante para la tecnología. De igual forma, años mas tarde, gente como Bill Gates o Paul Allen hicieron algo interesante con sus conocimientos.

Sin embargo estas hazañas nunca fueron consideradas como el inicio del Hacktivismo.

Según Bruce Sterling, el inicio fue cuando el 15 de enero de 1990, la centralita de larga distancia AT&T se vino abajo, dejando fuera de servicio a miles de abonados. Esto denota cierto interés por las catástrofes creadas por algunos Hackers, mas que por sus conocimientos. Sea por sus hazañas o por su afán de protagonismo, lo cierto es que ya hay un árbol genealógico de los Hackers más famosos, que de alguna manera han marcado la historia.

1.3. El árbol genealógico de los Hackers

Es difícil establecer un orden en este sentido, pero lo voy a intentar. Es obvio que Hackers, los ha habido, y muchos, mas de los que se mencionan en los diversos libros que se escriben sobre Hackers. Pero en algo se coincide en todos ellos. En que se barajan los nombres de los más importantes, o al menos, los que se han dado a conocer por sus hazañas.

En un árbol genealógico, bastante sencillo, tratare de encadenar cada uno de estos personajes. Estos hombres podrán ser considerados buenos o malos. Aquí no voy a hacer distinciones. Solo me argumentare en catalogarlos por un orden cronológico, no por sus proezas o ataques. En esto no voy a culpar a nadie.

1.4. Richard Stallman

Stallman brilla por su gran capacidad para programar. Todavía a día de hoy utiliza para trabajar, una maquina bastante antigua. Se trata de una DEC PDP-10. Stallman se integro en el laboratorio de Inteligencia Artificial del MIT en 1971, lo que le valió para crear sus propias aplicaciones de Inteligencia Artificial. Stallman, por sus trabajos, fue recompensado con el premio McArthur Genius. En la actualidad Stallman se dedica a crear miles de utilidades gratuitas para entornos UNIX. Evidentemente, no los escribe el solo, para ello creo recientemente la Fundación Free Software en la que intervienen muchísimos programadores.

1.5. Dennis Ritchie, Ken Thompson y Brian Kernighan

Estos tres mosqueteros del chip son buenos programadores y trabajan para Bell Labs.

Es como si esta empresa sólo gestara buenos Hackers. Los tres están especializados en el entorno UNIX y en el lenguaje C. Estos hombres han tenido que

ver, y mucho, con el nacimiento de Internet y su progreso. De no haber estado ellos en este proyecto, Internet quizás no existiría ahora, o de hacerlo, seria muchísimo más lenta.

En la actualidad Ritchie esta trabajando en el Plan 9 de Bells Labs, un sistema operativo de ultima generación que vendrá a sustituir a UNIX. Thompson y Kernighan todavía siguen trabajando como Hackers, algo que siempre les motivo a seguir viviendo con cierta ilusión.

1.6. John draper

Conocido como el capitán Crunch, este hombre fue quien descubrió que con un silbato de los cereales Crunch se podía hacer Phreaking. Este silbato curiosamente generaba un silbido a 2.600 Hertzios. Esta frecuencia es la que se empleaba para cortar los contadores de los teléfonos de Bell. Este descubrimiento llevó a John a crear la primera «Blue Box» una caja electrónica mágica para los teléfonos.

1.7. Paul Baran

Hay quien lo cataloga como el mejor Hacker de todos. Esto es solo una objeción de otro Hacker bastante conocido, Anonymous. No obstante hay que reconocer que Baran estuvo enredado con Internet incluso antes de que esta existiese como tal, por lo que los principios de Internet se deben asignar a Baran.

Baran comenzó a edificar lo que es hoy día, un Navegador. Baran tuvo un gran acierto con crear esta herramienta que a día de hoy, esta siendo utilizada por millones de internautas de todo el planeta.

1.8. Eugene Spafford

Este profesor de Informática de la universidad de Purdue, ha descubierto e impulsado a varios estudiantes realmente brillantes, entre los que destaca Dan Farmer. Spaffor es el creador de COPS «Computer Oracle Password and Security System», un sistema de seguridad para Redes.

1.9. Dan Farmer

Dan Farmer participo en la creación de COPS iniciado por el profesor Stafford, dado que Farmer era el alumno de Stafford mas destacado. Finalmente COPS vio la luz en 1991 y Farmer estaba trabajando para la CERT «Computer Emergency Response Team» de la Universidad Carnegie Mellon.

Farmer gano la fama al desarrollar SATAN «System Administrator Tool for Analyzing Networks», una herramienta realmente potente que sirve para analizar los defectos y los puntos débiles de una red remota.

1.10. Mark Abene

Con el alias Phiber Optik, este Hacker es uno de los miembros fundadores del grupo «Master of deception» un grupo dedicado exclusivamente al conocimiento profundo de los teléfonos. Su primer acercamiento a la tecnología fue con un Conmodore 64 y un sistema de Radio Shack TRS-80.

1.11. Johan Helsingius

Alias Julf, es el más popular creador de correo anónimo, es decir, él fue quien creó este tipo de correo seguro a través de una cuenta llamada *penet.fi*. Julf se inició con un 486 con 200 megas de disco duro.

1.12. Wietse Venema

En la actualidad, este hombre trabaja en la Universidad de Tecnología de Eindhoven.

Es un programador prolífico que ha recibido multitud de reconocimientos por todo su trabajo. Venema es coautor con Dan Farmer de la herramienta SATAN. Pero fue el programa TCP Wrapper, el que le lanzó a la fama. Esta herramienta de seguridad es una de las más utilizadas en el mundo. Este programa controla y registra los paquetes que entran en una Red. Evidentemente, esto le mereció un premio a su trabajo.

1.13. Kevin Mitnick

Mitnick es la leyenda viva. Se le conoce como el cóndor. Este apodo surge por la habilidad de este, de ser el más escurridizo del FBI. Es el Cracker más famoso del mundo. Kevin comenzó sus andanzas con tan solo 10 años. Con esta edad, Mitnick fue capaz de violar el sistema de seguridad del sistema de defensa de los EE.UU. Sus principios se basan en el Phreaking, desde entonces ha violado todos los sistemas de seguridad imaginables, incluyendo los militares, empresariales o las grandes firmas.

Su obsesión por recuperar un software de OKI, le llevo a invadir los ordenadores Tsutomu Shimomura en una noche de navidad. Shimomura era también otro Hacker.

Esto le llevo a la ratonera más grande jamás creada. En la actualidad Mitnick a cumplido condena y se encuentra libre, eso sí, le esta prohibido acercarse a un ordenador. Sin embargo se sabe que Mitnick actuó como asesor de seguridad contra el famoso Virus I Love You.

1.14. Kevin Poulsen

Este hombre siguió los mismos pasos que Mitnick. A Poulsen se le conoce por su gran habilidad para controlar el sistema telefónico de Pacific Bell. Una buena prueba de ello, es que Poulsen utilizo su talento para ganar un Porsche en un concurso radiofónico. Para ello intervino las líneas telefónicas, dándose prioridad asimismo. Pulsen ha violado prácticamente todos los sistemas de seguridad, pero parece que tienes mas interés en conocer los sistemas de la defensa militar. Esta filosofía le ha llevado a pasar por la cárcel, donde cumplió una condena de cinco años. En 1996 fue soltado y parece que hasta la fecha, Poulsen no ha hecho ninguna de las suyas, al menos que se conozca.

1.15. Justin Tanner Peterson

Justin Tanner es también conocido como el Agente Steal. Su habilidad haciendo cracking le llevó a conocer perfectamente las tarjetas de crédito. Pero no empleo sus conocimientos sólo para fines educativos, ya que lo que verdaderamente le motivaba, era ganar dinero de una forma rápida y fácil. Esta falta de ética del Hacker verdadero, le llevo a una sucia jugada con el FBI para trabajar con ellos en la clandestinidad. Su colaboración con ellos, le llevo a denunciar entre otros Hackers, a Poulsen, pero al final fue incapaz de protegerse el mismo.

1.16. Vladimir Levin

Vladimir Levin, un matemático ruso de 24 años, penetro vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citibank en Wall Street.

Una vez dentro, este Hacker logró transferir a diferentes cuentas de EE.UU, Rusia, Alemania, Israel y Suiza fondos por valor de 10 millones de dolares. Pero finalmente el Hacker fue detenido en 1995. En Internet es fácil encontrar un documento titulado «Como robe 10 millones de dólares".

1.17. Los escritores del Ciberpunk

También los escritores del Underground han tenido un antes y un después, y por supuesto un inicio. A ellos también se extiende este estudio. Un árbol genealógico nunca estaría completo sin los escritores que se encargan de resumir las actuaciones de los Hackers. Dentro de este grupo, podemos encontrar a los visionarios y los narradores de historias. De este estudio se extraen dos escritores. Se trata de William Gibson y Bruce Sterling, evidentemente no son los únicos, pero si los que han marcado un inicio.

William Gibson es el primer escritor que a acuñado el termino CiberPunk y que de hecho ha escrito sobre él. Su primera novela, Neuromante, esta considerada como el principio del movimiento CiberPunk. Nacido en 1948 en Myrtle Beach, South Carolina, Gibson imagino como serian los rebeldes del futuro. Todas las visiones que Gibson ha tenido, parecen cumplirse a rajatabla. Los Hackers de hoy, son quizás, una clara imagen viva de las premoniciones de Gibson.

Pero esto era pura ficción, así que Bruce Sterling toma la pluma e introduce un nuevo concepto de literatura. Sterling escribe La caza de Hackers y describe en su obra toda una persecución de Phreakers y Hackers. Dicha obra, para tomar mas relevancia, es publicada gratuitamente en Internet. Esta decisión, es la que ha llevado a Sterling a ser reconocido uno de los escritores mas acertados del Underground.

También el cine se ha hecho eco de la nueva sociedad CiberPunk, por un lado adaptando algunos libros de Gibson y por otro, creando todo un clásico del cine, Hackers, es el titulo de la película que cuenta las aventuras de un puñado de jóvenes Hackers que deben enfrentarse al FBI y al mas temido Hacker que esta del lado de la

seguridad de los EE.UU. La historia esta bien lucida y ya es un clásico entre los seguidores del movimiento CiberPunk.

1.18. El cine también habla de Hackers

No podía haber dos sin tres. Primero se ha hecho un retrato del árbol genealógico de los Hackers, de una manera básica y lo más cercana posible. Después se han mencionado a dos de los escritores del ciberpunk, más conocidos. Ahora cabe recordar aquí, en unas pocas palabras, que el cine también ha dejado un hueco para estos genios de la informática.

Después de recordar que la película más popular entre la comunidad Hacker, es precisamente Hacker, cabe recordar que también existen otras películas que abordan el tema del Hacking. En este sentido cabe recordar *The Ne*t «La ReD» de Sandra Bullock, una experta en Virus informáticos que es perseguida por otros Hackers.

Pero las películas que más extrañan son sin duda *WarGame* «Juegos de Guerra» y *Sneakers* «Fisgones» las cuales dan una clara idea de lo que es un Hacker y de lo que es capaz de hacer. Finalmente cabe destacar *The Matrix*, una película donde se muestran los Hackers del futuro, de ser esto último cierto, ¿Es posible que el mundo este dominado algún día por los Hackers?

Capítulo 2 La nueva Cibersociedad, los clanes de la ReD

La prensa está plagada de espectaculares noticias sobre estos individuos y otros que a menudo son confundidos con ellos. Nos estamos refiriendo a las grandes columnas que narran los hechos de un grupo de estudiantes que ha extendido una red de difusión de copias de programas informáticos. A estos individuos se les denominan de forma acertada, piratas informáticos, pero otras plumas se adelantan al describirlos como Hackers. Nada mas lejos de la realidad.

En el presente articulo trataremos de separar cada uno de los componentes que forman la nueva sociedad Underground con el fin de identificarlos correctamente y conocerlos a fondo. Es posible crear un perfil de cada uno de ellos y conocer cuales son sus intenciones a partir de las experiencias adquiridas en este sector. También trataremos de acercarnos mas al verdadero mundo del Hacking y que sucede en realidad en este terreno, por ello relataremos una crónica del Hacker, esto es, un día cualquiera de alguien que irrumpe la red con ganas de divertirse.

También es cierto que la nueva cibersociedad surge a partir de la era de la informática llevada al hogar, esto es así ya que la posibilidad de manejar un ordenador ha aumentado de forma considerable al ser altamente asequibles estos equipos. Por otro lado Internet ofrece con mucho, grandes posibilidades de exploración de mundos desconocidos y el encuentro con Software especifico, véase Sniffers o unabombers por ejemplo.

El acercamiento para cualquiera de la tecnología de los bits y las comunicaciones, ha despertado el interés de muchos talentos que son capaces de hacer algo mas que escribir un texto. Un ordenador presumiblemente podrá hacer un renderizado complejo de una imagen 3D, pero también es cierto que si conocemos el lenguaje a fondo, podemos hacer mas cosas que escribir o dibujar. Por otro lado hay que añadir, que cualquier programa de comunicación, como un navegador o un gestor de correo, siempre tendrá «una puerta trasera» por la que realizar otras operaciones que las permitidas. A esto se les denominan Bugs, pero nos preguntamos si acaso están hay de forma intencionada, ya que es difícil creer que una cosa así, pase inadvertido por cientos de ojos, ya que un núcleo o programa normalmente no lo realiza una sola persona.

Sea cual sea la razón, lo cierto es que estos bugs han permitido un aumento considerable de «cerebros fugados» capaces de detectarlos y hacer uso de ellos, algunos de ellos de forma indebida. Y estos «cerebros» han encontrado también una buena fuente de inspiración en la Red de Internet, ya que a través de ella se realizan los grandes Hacks y comprometen la seguridad del internauta aislado.

2.1. El perfil de un Hacker

Un Hacker es a todas luces, alguien con profundos conocimientos sobre una tecnología. Esta puede ser la informática, electrónica o comunicaciones. El Hacker normalmente conoce todos los terrenos en los que reposa la actual tecnología. Así pues, el verdadero Hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta mas difícil de descifrar. Nos estamos refiriendo a sistemas de cifrado o sistemas de codificación. En la actualidad los sistemas de cifrado y codificación están al orden del día, tomemos como ejemplo los canales de televisión de pago o cualquier soporte de grabación de datos como el CD o DVD.

Cada uno de estos dispositivos se basa en un estándar de codificación de datos, al igual que sucede con el protocolo de comunicaciones de Internet TCP/IP. En la actualidad y más en el futuro, la tecnología se basa en protocolos y datos correlacionados en cadena. El entendimiento de estas cadenas de datos nos darán una superioridad de control sobre cualquier tecnología. Este entendimiento nos permitirá entre otras cosas, modificar la información, un reto para todo Hacker.

Así un Hacker busca, primero el entendimiento del sistema tanto de Hardware como de Software y sobre todo descubrir el modo de codificación de las ordenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema.

El perfil del Hacker no es el típico chalado de los ordenadores que vive solo y para los ordenadores, aunque si es cierto que pasa largas horas delante de el. Ya que sin trabajo no hay resultados. Los conocimientos que adquiere el Hacker son difundidos por el, para que otros sepan como funciona realmente la tecnología.

Otros datos erróneos sobre la descripción del Hacker, es aquella que los presenta como adolescentes de gafas negras de montura de hueso y extendido acné sobre su cara, en la mayoría estudiantes de informática de cuerpos endebles que siempre consumen cocacola y pizzas. Esto es totalmente incierto, si bien podría coincidir en alguna ocasión, el Hacker normalmente es una persona normal con aspecto físico variado, estudiante de informática o no, al que le guste la cocacola o no. El Hacker puede ser adolescente o adulto, lo único que los caracteriza a todos por igual, son las ansias de conocimientos.

Tampoco es cierto que el Hacker surge a raíz de la nueva era de la informática, ya que Hacker es aquel que trata de averiguar cosas y esto se puede aplicar en las comunicaciones que existieron mucho antes que los ordenadores. De modo que se desmiente que los HACKERS tengan una edad temprana. Ya en la segunda guerra mundial se trataba de descifrar los mensajes del enemigo.

Sin embargo, también es cierto que es ahora, cuando mas proliferación de

Hackers existe, dado la importancia que cobra la informática y la Red de Internet hoy día. Por otro lado en la actualidad existe mas información al respecto a través de la prensa y WEBs en la red.

Los verdaderos Hackers aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes.

2.2. La nueva cibersociedad

A raíz de la introducción de la informática en los hogares y los avances tecnológicos que esta aporta, a surgido toda una generación de personajes mas o menos peligrosos que difunden el miedo en la Red y la prensa.

Catalogados todos ellos como «piratas informáticos» la nueva generación de «rebeldes» de la tecnología aportan, unos sabiduría y enseñanza y difunden, otros destrucción y desolación. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

Hasta la fecha esta nueva cibersociedad, ha sido dividida en una decena de grandes áreas fundamentales en las que reposan con fuerza, la filosofía de cada uno de ellos. Todos y cada uno de los grupos aporta, en gran medida algo bueno en un mundo dominado por la tecnología, pero esto, no siempre sucede así. Algunos grupos rebeldes toman estas iniciativas como partida de sus actos rebeldes.

Los hackers son el principio y el nivel mas alto de toda esta nueva sociedad. Estos poseen mayores conocimientos que el resto de grupos, pero emplean metodología poco agresivas para mostrar sus conocimientos. Los crackers son probablemente el siguiente escalón y los que son capaces de Crackear sistemas y romper su seguridad, extendiendo el terror entre fabricantes y programadores de Software. Los Lamers, auténticos curiosos aprendices de brujo, poseen mayor influencia en la red a través de WEBs espectaculares, pero vayamos por partes y tratemos cada grupo por separado.

Hackers: El primer eslabón de una sociedad «delictiva» según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de «he estado

aquí» pero no modifican ni se llevan nada del ordenador atacado.

Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso.

Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Crackers: Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica. Mas adelante hablaremos de los Cracks más famosos y difundidos en la red.

Lamers: Este grupo es quizás el que mas numero de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro ordenador, le fascinan enormemente.

Este es quizás el grupo que mas peligro acontece en la red ya que ponen en

practica todo el Software de Hackeo que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un «bombeador de correo electrónico» esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se mofa autodenominandose Hacker.

También emplean de forma habitual programas sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el ordenador esta apagado.

Toda una negligencia en un terreno tan delicado.

Copyhackers: Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año mas de 25 000 millones de pesetas sólo en Europa. En el año 1994 los Copyhackers vendieron tarjetas por valor de 16 000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los «bucaneros» personajes que serán detallados mas adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello «extraen» información del verdadero Hacker para terminar su trabajo.

La principal motivación de estos nuevos personajes, es el dinero.

Bucaneros: Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros solo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros solo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos «Crackeados» pasan a denominarse «piratas informáticos» así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a nivel masivo.

Phreaker: Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su

procesado de datos.

Newbie: Es un novato o más particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

Script Kiddie: Denominados Skid kiddie o Script kiddie, son el último eslabón de los calnes de la Red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack. En realidad son devotos de estos temas, pero no los comprenden.

Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los ficheros Readme de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propio ordenador. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los «pulsabotones» de la ReD. Los Kiddies en realidad no son utiles en el progreso del Hacking.

2.3. El Underground final

Se ha descrito brevemente cada grupo y supongo que habrá quedado claro quienes son cada uno de ellos y que papel interpretan en la nueva cibersociedad.

Son cada vez mas los jóvenes que se autodenominan Hackers y lo unico que hacen es soltar Virus y probar programas de Hacking. Esto confunde a la sociedad y este tipo de personas si son algo violentas y abolecen lo material. Disfrutan «fastidiando» al vecino y muestra una cara de idiota brillando bajo la luz de la bombilla, cuando suelta uno de esos fatídicos Virus o gusanos en la Red.

Los buenos Hackers, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema demasiado seguro. Entonces la han fastidiado.

Pero volviendo a la consideración de sí son una nueva sociedad difícil de

comprender, debo decir que así es, y también debo aceptar, al igual que todos vosotros que el verdadero Hacker posee el control del mundo.

Por ello alguien muy importante en los Estados Unidos dijo alguna vez, dadme diez Hackers y dominare el mundo. En otro margen de cosas, y tras conocer cada uno de los pobladores de la Red, en las siguientes líneas, daremos respuesta a 32 preguntas mas frecuentes y que terminaran de generalizar los conceptos de Hacker, Hacking y Seguridad en la ReD.

2.3.1 Que es un hacker?

Ha quedado bien claro en la primera parte de este articulo lo que es un Hacker, pero es obvio que vamos a reincidir en dejar claro lo que es un Hacker, por aquello de quien ha pasado directamente a esta sección.

La palabra Hacker definía, en una primera versión «después de la traducción de Hack» a los entusiastas de los ordenadores que permanecían largas horas de delante de ellos. En la actualidad se definen como expertos en programación y conocimientos elevados sobre informática y electrónica.

Por otro lado, la ley e incluso los medios escritos, aluden a esta nueva generación como aquellos que lindan con lo ilegal. En la actualidad, al fin, se describen a estos personajes como auténticos expertos en sistemas digitales que disfrutan explorando sistemas y probando sus capacidades en oposiciones los simples usuarios, que se conforman con redactar unas cuantas líneas en un procesador de texto.

2.3.2 Es seguro internet?

De todos es sabido que no. Hoy por hoy, la red de redes contiene mas virus, exploits, comandos javas «especiales» y otras especias que páginas WEB existen. Es

una paradoja, pero lo cierto es que tienes que andar con cuidado en la red. Los canales IRC suelen estar infectados de «aprendices» que emplean todo tipo de «armamento» IRC para fastidiar a cuantos chatean en el canal.

El correo electrónico también se ve perjudicado ya que puedes encontrarte un mensaje sin sentido que lo único que ha hecho es colocarte un «troyano» en tu ordenador o quizás un Virus. Para los usuarios que se decantan por el tema de Hacking, navegar sin precauciones por estas paginas, puede resultar peligroso, ya que a veces cuando se hace una descarga de algún programa, este contiene un virus o un troyano.

El pago electrónico a través de la red también esta en peligro, ya que existen programas específicos para interceptar las transiciones o en el peor de los casos emplean tu numero de tarjeta para futuras compras ajenas.

También existen utilidades que permiten escanear los puertos de cualquier ordenador conectado a la red y utilidades que controlan todos los paquetes que viajan por la red, sin embargo también es cierto que podrás navegar, a menudo, por la red sin tener problemas.

2.3.3 Esta bien visto ser hacker?

Para la sociedad no. Y de esto tiene la culpa en parte la prensa escrita, ya que a menudo se confunden los hackers con piratas informáticos. Por otro lado solo aparecen publicados las fechorías mas sonadas de la actualidad, como la penetración de piratas informáticos en el pentágono o la NASA.

O quizás han sido unos Hackers…lo cierto es que sólo publican el daño que han hecho, además en la actualidad se esta poniendo de moda el ciberterrorismo en la red, donde cuelgan severas protestas en las WEBs mas importantes.

Por otro lado la palabra Hacker parece estar ligada siempre a alguien que ha perpetrado un robo a un banco desde un ordenador o alguien que hace daño a cualquier internauta u empresa. La poca o mala información sobre el tema, y la expansión de nuevos «especímenes» en la nueva cibersociedad, infundan confusión.

2.3.4 Existen solo los hackers o hay alguien mas en la red?

Por supuesto que existe alguien mas, por ello la causa de la confusión del verdadero rol de los Hackers. Después de estos, están los Crackers Hackers de élite rebeldes que emplean sus conocimientos para difundirlos en la red en forma de Software que otros utilizaran indebidamente. Los Crackers revientan sistemas y roban la información del ordenador ajeno.

También están los Lamers o Newbies, esto es, novatos que se bajan de las paginas de otros «aficionados» programas Sniffers, escaneadores o virus para luego ser empleados a uso de ratón, ya que hoy por hoy no hace falta ser un experto programador para dirigir el puntero del ratón sobre cada pestaña del programa descargado.

Pero el grupo que mejor merecido tiene, son aquellos que no se denominan Hackers, como cuartango, en este caso son expertos en seguridad que detectan fallos o bugs en los sistemas y lo hacen publico, para que las empresas de dicho software «dañado» ponga remedio. Un ejemplo de ello, es el agujero de Cuartango, un bug o puerta trasera del conocido navegador EXPLORER que permite mediante una simple opción, coger información del disco duro de un ordenador remoto.

2.3.5 Que es un mailbonbing

Es el envío masivo de correo electrónico comúnmente conocido como bombardeo en el entorno del Hacking. Los MAILBONBING son programas que permiten enviar miles de veces un mismo mensaje a una determinada dirección de correo electrónico. A veces el mailbombing, también permite el envío de correo fantasma, esto es, correo falso sin dejar rastro para quien lo envía, esto le permite pasar inadvertido. A esto se le llama correo anónimo.

2.3.6 Que es un cracker

El tema Cracker también ha quedado suficientemente claro, pero podemos recordar de nuevo que se trata de un Experto Hacker en cuanto conocimientos profundos de programación y dominio de la tecnología.

El Cracker diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros ordenadores remotos. Muchos Crackers «cuelgan» paginas WEB por diversión o envían a la red su ultima creación de virus polimorfico.

También existen Crackers que se dedican a crear Cracks para Software importante y negocia con ellos, existen cracks para tarjetas, Shareware y sistemas electrónicos como el DVD o las consolas Playstation entre otros.

2.3.7 Que es irc

Comúnmente conocido como canal de chateo o «forma de intercomunicarse con otros usuarios en tiempo real a través de texto y ahora voz» se ha convertido en un canal de guerra en el que entras para preguntar algo en concreto y recibes como respuesta una bomba lógica o un virus.

Existen multitud de herramientas IRC en las paginas de Hackeo y utilidades WAR o de guerra, es una moda ir fastidiando por este canal.

2.3.8 Que es un lamer

Es un aficionado en el tema. Es aquel que ha visitado varias paginas WEB sobre Hacking y se ha bajado unos cuantos programas fascinados. Después hace uso de ellos indebidamente y sin conocimientos, lo mismo se destruye su propio ordenador

como otros de la red y cuando esto sucede se siente alguien superior a los demás.

Este tipo de personajes es quien emplea los Bac Orifice, Netbus o virus con el fin de fastidiar y sin tener conocimientos de lo que esta haciendo realmente. Son el ultimo escalón de la nueva cibersociedad.

2.3.9 Son seguras las paginas web sobre hacking

Algunas de ellas pueden resultar peligrosas e inseguras, pero no todas. Es cierto que las paginas sobre Hacking, pueden resultar una muy buena fuente de información para los «novatos», pero existen algunas paginas, creadas por personas con vagas intenciones, que colocan en ellas utilidades dañinas como Virus o cookies «malos».

Un ejemplo esta en lo que me sucedió el otro día. No recuerdo que pagina era, pero si que aparecía tras una búsqueda en el buscador METABUSCA. En ella aparecía una pagina que llamaba la atención por su aspecto gráfico. Cuando trataba de bajar un archivo de no mas de 30 Kbytes y justo cuando estaba al 95 % de la descarga, la utilidad de Antivirus de Panda Software detectó un virus solicitando abortar o desinfectar.

Seleccione desinfectar y la sorpresa fue cuando un nuevo cuadro de dialogo me indico que era imposible desinfectar el fichero. La única solución era pulsar escape, pero ya era demasiado tarde, el nuevo virus con nombre desconocido VxD y unos cuantos números aleatorios, había resultado ser un programa autoejecutable, que terminó por bloquear el ordenador.

Lo curioso del caso es que después de resetear el ordenador este no detectaba el fichero principal del Antivirus panda. Tras arrancar Windows, Panda había dejado de funcionar porqué el fichero EXE había sido borrado del sistema. Pero lo que más me impacto fue cuando trate de instalar de nuevo el Antivirus.

Este ya no se podía instalar de nuevo, abortándose el proceso de instalación.

2.3.10 Que es un troyano

Un troyano posee diversos significados y acometidos. Atrás, un troyano era un programa oculto que proporcionaba un cuadro de dialogo falso que debías aceptar, tras lo cual, el troyano se «quedaba» con lo que tecleabas después, en este caso la clave. Después el troyano encriptaba la clave nuestra y se enviaba de forma automática a un correo electrónico especifico, cuando empleábamos el correo electrónico, sea cual sea la dirección.

Ahora un Troyano recibe el nombre de Back Oríifice, Netbus o Deep Troaht. Estos troyanos se dividen en dos grandes bloques, un servidor y un cliente, ambos ejecutables. Colocando el fichero servidor a un ordenador remoto y ejecutando nuestro cliente podemos controlar cualquier función del otro ordenador.

Estos, son los troyanos que han hecho «flaquear» la seguridad de Windows 95 o 98.

2.3.11 Que es una bomba lógica

Es lo mas parecido a un virus. Una bomba lógica es un programa autoejecutable que espera un determinado tiempo o actividad sobre el teclado para explotar, o dicho de otra manera, infectar el ordenador, modificando textos, mostrando gráficos o borrando parte del disco duro.

2.3.12 Es seguro el correo electrónico

En absoluto, el correo electrónico no es nada seguro. A través de él se pueden recibir ficheros «pegados» indeseables. Además el correo electrónico puede ser interceptado y leído por los Lamers, que emplean Sniffers, programas capaces de

interceptar correo electrónico entre otros.

2.3.13 Que es un firewall

Un Firewall es una utilidad o herramienta de seguridad, que impide que ciertos comandos o paquetes de datos «anormales» penetren en nuestro sistema. Comúnmente son traducidos como barreras de fuego, que detectan ataques o entradas forzadas en los puertos de nuestro sistema. Denominados también Nuke.

2.3.14 Son seguros los dowloads desde internet

Ni mucho menos, entre ellos puedes descargar un virus «insertado» en el programa o un troyano renombrado. Las descargas más peligrosas son las extensiones ZIP y EXE. El servidor de Back Orífice, puede renombrarse fácilmente y hacernos creer que estamos bajando otro fichero.

2.3.15 Es seguro windows 95 o 98

Con la presentación en sociedad de Back Orífice por «Cult of The dead» Windows ha dejado de ser un sistema operativo aislado y seguro por sus limitaciones de comunicaciones en redes, excepto el explorador.

En la actualidad se han encontrado bugs en el navegador que permiten a alguien

husmear nuestro disco duro o robar ficheros de nuestro ordenador. Es el denominado agujero de cuartango, el bug más peligroso de todos.

Los cookies de las paginas WEB son otra amenaza para Windows, pero como mucho nos cuelan algún tipo de virus. Sin embargo lo más peligroso es el fichero servidor.EXE de Back el que hace tambalear Windows, dada la moda reciente de «controles remotos».

2.3.16 Que es back orífice

Back Orífice es un programa de control remoto de ordenadores que funciona bajo un servidor y un cliente. si colocamos el servidor a otro ordenador remoto, es posible desde el cliente, gobernar cualquier función del ordenador remoto, entre los que destaca abrir y cerrar programas, controlar el CD, leer y escribir ficheros o borrar parte del disco duro.

Para ello el servidor sé autoejecuta y se borra cada vez que el ordenador ajeno se enciende, nuestro cliente escanea el puerto elegido y cuando este esta abierto, actúa a través de él, desde un menú cliente repleto de pestañas y opciones de control remoto. El sistema es bueno para controlar un ordenador o ordenadores en una red LAN interna y a pesar de lo que se diga, podría ser menos nocivo que un virus, aunque dejar esta puerta abierta para Windows es todo una amenaza.

2.3.17 Que es un pirata informático

Comúnmente confundido con un Hacker, un pirata informático es quien hace copias de Software en CD y comercializa con ellos. No posee conocimientos, mas que para duplicar discos y este es el grupo que más ensucia a la nueva sociedad de hackers, después de los Lamers.

2.3.18 Que es netbus

Se trata de un troyano anterior a Back Orífice y funciona bajo los mismos principios que este, en la actualidad esta siendo de moda el empleo de Netbus o Back Orífice por cualquier usuario de ordenador.

2.3.19 Existe un manual del hacker

Existen varios y todos ellos se encuentran en Internet. El manual del Hacker indica los diez puntos más importantes que todo buen Hacker busca en su progreso hacia la cumbre. Los manuales están en ingles, pero existen versiones reducidas en español, bajo el nombre de «novicio», estos manuales normalmente cubren situaciones dirigidas hacia los «nuevos» en esta cibersociedad y por supuesto no indican el modo de hacer funcionar programas peligrosos.

2.3.20— Que herramientas son imprescindibles para el «hacker»

El Hacker necesita herramientas que le faciliten el trabajo en la red. Entre estas herramientas destacan los sniffers, escaneadores y programadores de tarjetas inteligentes. También se recomienda poseer algún Mailbombing y Nukenabber para enfrentarse a aquellos que solo actúan por fastidiar.

Para entrar en sistemas ajenos, «aunque sea solo para ver dentro de el y salir después» el Hacker debe echar mano a un buen diccionario para obtener la clave de acceso. Actualmente también es necesario disponer de utilidades de guerra IRC y WAR, para enfrentarse a otros enemigos. Un buen Virus bajo la manga nos apartara al indeseado que nos moleste.

Pero lo más importante es la motivación y la intuición, sin ellas nada se puede hacer.

2.3.21— Que es pgp

PGP, de Pretty Good Prívate es el programa de cifrado por excelencia para la mayoría de usuarios que pretenden proteger su correo electrónico o ficheros de texto. Este programa que conoce numerosas versiones y mejoras, fue inicialmente desarrollado por Philip Zinmermam, quien tuvo sus encuentros con la justicia americana.

El programa de cifrado basado en RSA, o Diffie fue prohibido para su exportación, pero a alguien se le ocurrió publicarlo en Internet en forma de texto, y alguien lo compilo de nuevo en Europa. Así fue como PGP llego a Europa. Actualmente esta por la versión 6.0 e incluso se conoce una versión en castellano de este programa de cifrado altamente seguro.

También los hackers deben disponer de esta herramienta.

2.3.22— Que es warez

Warez es en realidad software «conocido» que lleva incluido un Crack para ser instalado sin numero de serie o en varias maquinas sin pagar por él. En Internet se encuentran infinidad de Warez y números de serie para los programas más conocidos. Los Warez son una forma de Crackear software y linda con el lado del delito entrando de lleno en él, ya que se violan los derechos de autor.

2.3.23— Que son los escaneadores

El mas conocido es el Scanerport y como su nombre indica, se trata de programas que permiten rastrear la red en busca de puertos abiertos por el cual acceder y manipular un sistema o introducir un troyano o virus.

PortScan es otra utilidad ampliamente conocida por los Hackers y con este programa nadie esta a salvo.

2.3.24— Que es un crack de software

El Crack de un software, que convierte al mismo en un Warez, es la inclusión de un código o varias líneas de códigos en los ficheros de registro del Software que impide que se caduque tal programa.

Todas las versiones de evaluación o Shareware poseen caducidad. Los datos que permiten esto, normalmente están encriptados y divididos en diversos ficheros DLL, REG e incluso INI. Cada programador oculta el código de tiempo donde le viene mejor. EL Crack consiste en alterar estos datos u otros de forma que el programa no reconozca la fecha de caducidad.

Por otro lado, el Crack es también la localización del numero de serie del programa. Este numero de serie es localizado gracias a un generador de números de serie o Generator, una utilidad muy ampliada por los Crackers para obtener logins o números de serie.

2.3.25 Es seguro el protocolo tcp/ip

El protocolo de comunicaciones de Internet TCP/IP es quizás, el protocolo menos seguro de cuantos existen, pero este es el estándar y por ello los Hackers desarrollan

continuamente herramientas capaces de monitorizar la secuencia de datos y paquetes TCP/IP.

SSL pretende ser un nivel de seguridad para transacciones electrónicas de dinero, pero también ha sido objeto de conocimiento de los Hackers y por tanto un sistema inseguro.

Los sniffers pueden monitorizar estos comandos, al igual que el VOYAGER monitoriza los comandos de las tarjetas ISO 7816.

Un protocolo seguro seria aquel que contenga protocolos variables y encriptados, así como estructura de paquetes variables.

2.3.26 Que es nukenabber

Es un programa que controla todos nuestros puertos y su estado y es capaz de detectar una intrusión o Nuke en cualquiera de los puertos seleccionados. En el caso de Back Orífice, podemos «vigilar» el puerto 12346 que es el empleado por este troyano y descubrir si alguien controla este puerto.

Nukenabber es una utilidad muy útil para un Hacker.

2.3.27 Que es el prheaking

El Prheaking es una extensión del Hacking y el Cracking. Los Phreakers son expertos en sistemas de telefonía fija o inalámbrica. Conocen a fondo los sistemas de tonos, enrulados, tarjetas inteligentes y el sistema GSM.

Tron era un buen ejemplo de Phreaker, ya que había logrado clonar una tarjeta GSM. Los Phreakers emplean sus conocimientos para realizar llamadas gratis y a veces es empleado por Hackers para mantener sus actividades en la red.

2.3.28 Que es un sniffer

Un sniffer es una utilidad que permite la monitorización de la red y detecta fallos de seguridad en ella o en nuestros sistemas. Dentro de los sniffers podríamos citar otras utilidades de control como KSA y SATAN, que además de buscar las debilidades de un sistema, son empleados como Sniffers, esto es, monitorizacion de la red y la unidad central.

Una navegación lenta en Internet nos puede indicar que hay un sniffer en línea.

2.3.29 Que es carding

El Carding es una extensión mas de esta nueva cibersociedad y sus constantes búsquedas por controlar todos los sistemas informaticos y electrónicos de la sociedad actual. Hoy por hoy la implantación de las tarjetas de crédito, es masiva y está presente en casi todos los sectores tales como operaciones bancarias, acceso a televisiones de pago, sistemas de pago electrónico y acceso controlado.

El Carding es el estudio de tarjetas chip, magnéticas u ópticas y comprende la lectura de estos y la duplicación de la información vital. actualmente se ha conseguido clonar las tarjetas GSM, tarjetas de canales de pago y Visa por este procedimiento.

2.3.30 Emplean la criptografía los hackers

Mas que nadie, los hackers o crackers se ven obligados a emplear sistemas criptograficos para su correspondencia electrónica. Normalmente emplean el conocido PGP, pero también es habitual otros métodos de cifrado, siempre de claves publicas. También es cierto que los Gurus emplean métodos criptograficos

desarrollados por ellos mismos, además del empleo de la esteganografia, método que permite encriptar datos en una imagen o gráfico.

2.3.31 Que son los diccionarios

Existen dos tipos de diccionarios entre la comunidad Hacker y ambos son imprescindibles dado su contenido. El diccionario básico del Hacker es aquel que detalla la extensión de los nuevos acrónimos habitualmente empleados entre esta sociedad. Así se describen acrónimos como spoofin, Nuk, Zombie o Crash entre otros. Para poder moverse entre la nueva sociedad es necesario saber el significado de cada uno de los acrónimos que permiten conocer a fondo todo lo relacionado sobre el Hacking, Cracking, Phreaking y otros servidores.

El otro gran diccionario y verdadera utilidad de los Crackers mas que de los Hackers, es el diccionario de palabras. cuando se emplea la fuerza bruta para obtener los Paswords o contraseñas de un programa, pagina WEB u ordenador remoto, es necesario y muy habitual emplear este diccionario, normalmente en formato Software.

El programa y/o diccionario electrónico compara miles de palabras hasta dar con la clave correcta, a esto se le denomina fuerza bruta ya que se compraran miles de palabras en menos de un segundo.

2.3.32 Que es la ingeniería social

La ingeniería social es quizás la base de un Hacker, para obtener los datos o lo que le interesa por medio de una conversación y de personas. Es la forma de engañar al otro, camelarlo y hacerle creer que eres alguien bueno, el técnico de la compañía de teléfonos quizás.

Una buena muestra de ello, es el timo de telefónica, en el que te llaman haciéndose pasar por un técnico de la compañía y te solicitan que teclees un número después de colgar. Este comando llamado ATT, le permite al ingeniero social, realizar llamadas a través de tu teléfono.

Y en la actualidad esta sucediendo en nuestro país, así que cuidado.

2.4. Los Clanes de la ReD y el futuro

En pocas páginas se ha resumido lo que es el argot del Hacker, así como quien puebla la nueva Superciudad que es Internet. Básicamente se han nombrado a todos, pero es evidente que los contenidos en la ReD van en aumento día a día, y es muy fácil que surjan nuevos vástagos en la gran familia de los clanes de la Red. La libertad de expresión, que permite Internet, en todos sus aspectos, despierta la curiosidad de miles de internautas nuevos cada día. La información se derrocha en este medio, y un internauta cualquiera puede accederá información «confidencial» en muchos aspectos, o información que antes era imposible de conocer.

Esta información permite al verdadero Hacker o aspirante a Hacker, a progresar en sus investigaciones, pulir sus técnicas o simplemente, mantenerse entre la elite. Pero también es cierto. Que tanta información permite a usuarios no aspirantes a Hacker, manipular tecnologías, que antes, solo eran accesibles a los técnicos o ingenieros de cada rama.

Por citar un ejemplo, en la actualidad es posible romper un sistema de televisión de pago, sin ningún tiempo de conocimiento. Esto es debido, a que existen páginas repletas de información de como hacerlo. Es mas, en realidad el usuario de la ReD puede permitirse el lujo de bajarse de la ReD ficheros que le permitirán ver canales de pago. No quiero citar aquí que canales, pero es de sobra conocido por todos. Esto implica que la rotura o el «Crack» del canal de pago se hace a diario sin demasiados conocimientos. Solo unos pocos conocen la tecnología y muchos son las que la ponen en practica de una manera sencilla.

Esto significa, que día a día se pueden formar nuevos grupos o personajes en la Red, que de alguna manera u otra hacen un uso diferente de estos conocimientos o información. Por de pronto todos los usuarios que toman un foro a diario, por ejemplo un foro que trata sobre los sistemas de televisión de pago, son los

denominados Kid Rapid, los denominados chicos rápidos, ya que con solo realizar unos cuantos clics de ratón pueden poner en practica un Crack complejo y sofisticado, como ver canales de pago de forma gratis y sin ningún esfuerzo.

Mas adelante, la posibilidad de nuevos vástagos en la Red y el Underground son infinitas. Así, el futuro de la Red y a sus pobladores, nos permitirá escribir unos cuantos capítulos más.

Capítulo 3 Historias de Hackers y Crackers

Tomemos un momento de descanso y repasemos historia. También es bueno analizar que han hecho algunos Hackers y Crackers, con el fin de inspirarnos un poco o impresionarnos otro tanto.

En las siguientes líneas explicare algunos sucesos, los cuales más me han impactado, pero estoy seguro que existen mas penetraciones de sistemas informáticos, Craks y toda una extensión de fechorías que no cabrían en este libro.

Me tomaré también la libertad de cambiar nombres y lugares de los hechos, por aquello de no «delatar» la intimidad si así no se desea, pero claro esta si un buen día se escribió sobre ellos, a modo de título les gustaba salir en la prensa, pero siempre había una pequeña nota, bajo el articulo que decía:

> Los nombres y lugares de los hechos son ficticios, pero los hechos, son por el contrario, reales a todas vistas.

Ahora la prensa se entera de si tu perro se mea en el sofá. Pero, por mi parte y con mucho respeto no diré si el perro de un buen Hacker se mea en el sofá, ni tampoco revelaré su nombre. Simplemente expondré algunos sucesos, que simplemente, no han pasado desapercibidos. Entonces, vamos alla!.

3.1. El caso del Phreaker ciego

Es quizás, y con toda probabilidad la historia que más me ha impresionado de alguna manera. Se trata de Tim Rosenbaum, un chico que a la temprana edad de 10 años, acometió, lo que hasta la fecha será la mayor estrategia lograda.

El buen chico nació ciego, pero dios le dio un excelente sentido, el oído, con una sensibilidad superior a los demás seres mortales. Sus blandas yemas de los dedos también poseían un tacto inverosímil, capaz de almacenar el tacto suave o áspero de las cosas y reconocerlas por ellas después.

Y también tenia algo que fascinaba a todos los chicos de Dollan, un pequeño pueblo costero al este de Maine, y esto eran sus silbidos. Era capaz de imitar a los pájaros de todas las clases y sobre todo podía controlar el tono del silbido hasta alcanzar notas musicales, hasta que un buen día le sucedió algo realmente importante.

A Tim le encantaban los teléfonos y sobre todo le encantaba escuchar la voz del otro lado del hilo cuando alguien llamaba a casa. Cada vez que podía marcaba un número cualquiera de teléfono y se sentaba a escuchar la cálida voz que decía; Este número está fuera de servicio.

Hasta que un buen día Tim silbó al tiempo que la voz decía la frase y callo de golpe. Esto asombro a Tim. Volvió a marcar otro numero de teléfono, silbó y sucedió lo mismo. Años mas tarde descubría que era capaz de generar silbidos a una frecuencia perfecta de 2.600 ciclos, el tono que indica que el teléfono esta colgado.

De esta forma Tim fue catalogado como uno de los primeros Phreakers de la historia. Tras este descubrimiento algunos ingenieros electrónicos probaron diversas frecuencias y descubrieron que se podían activar y desactivar los contadores de las centralitas y realizar llamadas de larga distancia de forma gratuita.

Basándose en la generación de tonos, con osciladores estables, se creó la primera cajita azul, que fue rápidamente extendida por su buen funcionamiento, y sobre todo porque se podía llamar gratis con ella.

3.2. El robo del banco

Uno de los casos mas difundidos, quizás sea el que sigue; dos Hackers tenían como objetivo ganar dinero fácil y de forma rápida. El objetivo así, era una sucursal de Citibank, en nueva York.

Los dos Hackers descubrieron, mientras monitorizaban la Red, que esta sucursal realizaba las transferencias a través de una compañía telefónica, y el sistema empleado era una red X.25.

Descubierto esto los dos hackers decidieron que si podían monitorizar estas transacciones, también podían redirigirlas a otra cuenta. Claro que había que retirar el dinero antes de que se dieran cuenta. Haciendo manos a la obra, buscaron el prefijo de la sucursal. Probaron varios números en serie a partir de un par de prefijos que sabían de antemano, hasta que terminaron por conectarse con varias terminales VAX. Durante un fin de semana se dedicaron exclusivamente a penetrar en ellos.

Después de esto fueron deduciendo terminales hasta quedarse con cinco de ellos.

Sabían que uno de ellos era el que controlaba las transacciones. De estas terminales, una, parecía interesante porque tenia un debug o puerta abierta. Les fue

fácil entrar en ella, empleando la clave de acceso del fabricante, ya que se ve a nadie se le ocurrió cambiar esta clave.

El sistema al que accedieron contenía menús que los guiaban a través de cuentas bancarias. Después de varias horas de exploración, encontraron un paquete de herramientas que permitía crear directorios y programas. Los dos Hackers crearon uno, que interceptaba todas las entradas y salidas del terminal. Después crearon un directorio y decidieron que este fichero seria el capturador de las transacciones.

Varios días mas tarde accedieron de nuevo a este terminal, e impresionados vieron como esta unidad había hecho multitud de transacciones en los días anteriores. Descubrieron a su vez que este terminal se conectaba a otra unidad parecida y tras una petición recibía una respuesta, entonces se iniciaba una larga serie de números y letras como password.

Los Hackers grabaron estos datos y los emplearon días después, generando cientos de transacciones a una cuenta «ficticia» que ellos habían creado. Hasta aquí esto no era mas que una prueba de que sabían los datos de control de cada ordenador. De modo que se tomaron unos días de descanso y planearon el gran golpe.

Días mas tarde abrieron una cuenta en Suiza y otras seis en Estados unidos, donde residían. Cada cuenta estaba registrada a un nombre diferente. Cada una de las cuentas tenia una pequeña cantidad de dinero y tras extinguirse la noche, los Hackers pusieron manos a la obra.

Durante largas horas, los dos Hackers hicieron turno delante del terminal, respondiendo los acuse de recibo. Al mediodía tenían cerca de 200 000 dólares en sucuenta de Suiza y al final de la semana, cada uno se llevo 100 000 dólares en efectivo a casa.

Esto hoy día, es más difícil de realizar, pero no imposible, la historia parece haberse repetido en Hong Kong en los últimos meses, un Hacker japonés había robado las cuentas de mas de 200 000 clientes de un importante banco de ese país. Pero esta vez fue descubierto.

3.3. El primer virus

El primer Virus se le escapo a alguien o «lo soltó» deliberadamente en la Red, causando este un colapso en las comunicaciones. En realidad se trataba de un Worn o

gusano, como quiera llamarle. El creador se sorprendió de los efectos y tuvo que crear otro programa que anulara las funciones de este primero. Así nació, también el primer Antivirus.

Pero de todo esto se ha escrito mucho y según Paul Mungo y su colega Bryan Clough, el primer virus tuvo lugar el 22 de octubre de 1987. Este primer Virus infecto varios cientos de disquetes. Y en la prensa lo catalogaron como una catástrofe, hasta el punto que se llego a decir que se pedían 2.000 dólares para inmunizar o destruir este Virus. Los investigadores pusieron manos a la obra y descubrieron el mensaje «oculto», en realidad no se pedía dinero y como una forma de evadirse o justificarse, el creador del Virus mostraba un teléfono de contacto para poder solicitar lo que entonces se denominaba, «Vacuna».

Este Virus se llamó Brain y en realidad tampoco era demasiado destructivo, «comparado con los actuales». El Virus Brain se esconde en el sector de arranque del disco y espera a que el ordenador se ponga en marcha y lea las primeras pistas del disco. Entonces se carga a si mismo en la memoria RAM, como si este fuera un programa de arranque común o BOOT.

El virus Brain es excesivamente largo, comparado con los posteriores virus mas sofisticados, tenia una densidad de 2750 bytes, los cuales no cabían en el sector de arranque. Así, que el Virus hacia dos cosas; colocar sus primeros 512 bytes en el sector de arranque y almacenar el resto de datos en otras seis pistas del resto del disco. De forma que siguiera una cadena.Este Virus «conocido como el primero» podía resultar inofensivo a primera vista si el disco no estaba demasiado lleno, pero a la sazón si este estaba completo, el Virus, que se autoreplicaba, podía borrar algunos datos importantes, cuando este se reescribia en otras pistas del disco.

El Brain también tenia un contador, y trataba de infectar un nuevo disquete cada cierto tiempo. Esto era lo que realmente hacia peligroso al Brain, en manos inexpertas. La única misión que tenia este Virus era insertar la etiqueta de bienvenida, Brain y ejecutar un proceso automático de reescritura. Pero por aquel entonces los ingenieros le dedicaron más de una semana, en estudio y para erradicarlo totalmente.

Y ese fue el principio de una nueva generación de micro-programas autoreplicantes que implantarían el terror en los siguientes años, hasta llegar a la actualidad, en la cual se les consideran el mayor «terror de la Red».

3.4. Kevin Mitnick, el nuevo forajido

La historia de Kevin comienza a la temprana edad de 16 años. Corría el año 1980, cuando Kevin rompía la seguridad administrativa del sistema informático del colegio donde estudiaba. En aquella ocasión, solo se limitó a «mirar» los ficheros del sistema y no tocó nada.

Al año siguiente, Kevin en compañía de unos amigos, penetró físicamente en las oficinas de COSMOS de Pacific Bell. Esta era una base de datos de control de llamadas, y Kevin y sus amigos robaron algunos manuales del sistema, las claves de seguridad, la combinación de las puertas de acceso al lugar y dañaron otros tantos archivos. Por ello, después Kevin y sus amigos, «después de que la novia de uno de los amigos los delatara como autores de los hechos» eran condenados a tres meses en un centro de detención juvenil de los Ángeles y un año de libertad provisional.

Pero Kevin solo había hecho mas que empezar. En 1982 Kevin entró de forma ilegal en un servidor del ministerio defensa y en aquella ocasión, tuvo la precaución de modificar el fichero de rastreo de llamadas, para no ser localizado. Sin embargo, un año mas tarde si fue localizado y arrestado, tras entrar a través de Arpanet, a los ordenadores del pentágono. En esta ocasión fue condenado a seis meses en un reformatorio. Y fué a partir de aquí cuando Kevin, se convirtió en leyenda. El hecho de haber entrado y romper las barreras del «North América Air Defense Command Computer» le convirtió en el Cóndor y la nueva leyenda.

Pero como siempre dicen, la leyenda nunca muere y en 1988 protagonizó otra de sus andanzas. Esta vez Kevin cumplió un año de prisión por robo de Software. Todo comenzó cuando durante varios meses, Kevin observó el correo electrónico del departamento de seguridad de MCI y Digital.

Con la ayuda de un amigo, Kevin penetró en el sistema y capturó 16 códigos de seguridad de ambas compañías. Pero del ordenador principal de Digital, Kevin se llevó consigo los ficheros de un nuevo prototipo de seguridad S.O, denominado VMS. Esto fue lo que alerto a los ingenieros de Digital, que rápidamente se pusieron en contacto con la FBI y así fue como comenzó el rastreo hasta dar con Kevin.

En 1992 Kevin salía a la calle y comenzaba a trabajar para una agencia de detectives, que en un principio vieron en él, el perfecto hombre que resolvería importantes «cambios", pero pronto Kevin penetró en sistemas y más sistemas y el FBI, determinó que era Kevin quien estaba detrás de todo. Pero Kevin escapo esta vez.

Sin embargo es 1994, cuando Kevin conoce, lo que seria su caída mayor. Al estar «prófugo» de la justicia. Kevin no puede dar su identidad en ninguna parte, ya que esta, en busca y captura y como tiene que moverse, Kevin se hace de un portátil y un teléfono móvil, y es así como esquiva en cada ocasión a la policía y al propio FBI.

Como Phreaking, Kevin era un autentico especialista pero necesitaba algo más. Él sabia que existía el peligro inminente de ser detectado muy pronto. Eso lo sabia

porque empleaba un teléfono móvil motorola y como todos, estos poseen un software, «oculto» que permite enviar una señal a la central para su localización, pero Kevin sabia que los teléfono OKI, permitían «puentear» esta opción y sabia donde podría encontrar el Software para ello.

Así, la noche del 25 de diciembre de 1994, Kevin había penetrado en el ordenador de Tsutomu Shimomura, el hombre que lo capturaría un año mas tarde, en busca del Software de OKI. Un Software que también era «pirata» ya que Tsutomu era Hacker antes que experto de seguridad.

Nueve minutos después de las dos de la tarde del 24 de diciembre de 1994 Kevin, iniciaba la ardua tarea de entrar en los sistemas de Tsutomu, que estaba ese día fuera de su domicilio. Los tres ordenadores de la casa de Tsutomu en San Diego, California, comenzaron a recibir una serie de instrucciones externas. Kevin trataba de averiguar que relación tenían entre sí los tres ordenadores que estaban encendidos ese día y pronto averiguo cual de las maquinas era el centro de la pequeña red local.

Se trataba de una SPARC que había sido detectada en tan solo tres minutos. Después de una pausa, recibía una solicitud de conexión desde una dirección falsa de Internet. El ordenador SPAC contestó con la respuesta adecuada de conexión con la «dirección falsa».

Kevin ya estaba cerca de su objetivo, pero no respondió a la maquina y en lugar de ello, envió otras 29 peticiones más seguidas en los tres segundos siguientes. Con lo que consiguió bloquear la maquina con una ráfaga de datos velozmente transmitidos. Había conseguido su primer paso.

Después otra de las estaciones SPARC de Tsutomu que se empleaba como terminal, recibió otras 20 solicitudes en no más de diez segundos. El terminal reconoció cada una de ellas, pero siempre recibió un mensaje de cancelación, con el fin de despistar esta segunda maquina conectada a la red.

Pero más que despistar, Kevin lo que quería era «capturar» los datos obtenidos como respuesta de estas estaciones SPARC. Estudió cada una de estas respuestas y dedujo que debía añadir 128 000 unidades al número de respuesta. De esta manera Kevin podía acceder al tercer terminal. Tras esto, Kevin añadió un fichero «oculto» que le permitiría entrar libremente cada vez que lo solicitara, sin tantas complicaciones como esta vez.

Kevin husmeo el disco duro y encontró algo que le interesaba. Era el software del OKI y otros tantos archivos de seguridad que Tsutomu había desarrollado. Y esto fue lo que realmente cabreó e incitó al japonés afincado en Estados Unidos, a iniciar una persecución lenta y laboriosa que concluyo el 15 de Febrero de 1995, con la captura de Kevin y su nuevo «Teléfono fantasma».

3.5. El caso del sistema de codificación de videocrypt y el profesor ZAP

El caso más sonado es quizás el que le sucedió al grupo SKY y su sistema de codificación Videocrypt. Dicho sistema se anuncio como el más seguro y se creó con la intención de frenar la actividad febril de los piratas, en una época en donde todo se codificaba por métodos analógicos y por tanto eran fácil de clonarse. Careciendo en todo momento de una seguridad absoluta o fuerte.

El nuevo sistema de Videocrypt aumentaba su seguridad ya que se basaba en tecnología digital para la codificación de vídeo. Ademas presentaba una importante novedad, y es que el nuevo sistema de encriptación se basaría en una tarjeta de acceso inteligente. Un punto fuerte según los ingenieros que lo inventaron. A partir de ahora se podría activar y desactivar cada descodificador a voluntad. Ademas el sistema digital de encriptación permitía trabajar con algoritmos complejos y estos necesitaban de claves secretas que se albergaban en el interior de la tarjeta electrónica.

Sin embargo no tardarían en descubrir que la orden de activación se definía como una tensión de control sobre el descodificador. De modo que bastaba con cortar una pista de cobre del circuito o Hardware del descodificador para eliminar la función de activación y desactivación del sistema. Y por supuesto el sistema más fuerte había caído repentinamente.

No obstante sé tenia en cuenta dicha posibilidad y rápidamente entró en acción la segunda fase. A partir de ahora el sistema se complicaría aún más. El algoritmo del embrollamiento se trataría en el interior de la tarjeta y la orden de activación y desactivación del equipo descodificador, ya no seria una simple tensión de control. A partir de ahora se convertiría en una palabra u octeto en forma de respuesta a partir de una palabra más larga. Dos claves, una pública y otra secreta se encargarían de desentrañar la clave de acceso. Así la clave pública se desenmascaria en el interior del descodificador, mientras que la clave secreta se revelaría en el interior de la tarjeta de acceso.

De esta forma si se pretendía hacer un Hack sobre el sistema seria por vía software a partir de ahora y no por Hardware como había sucedido en un primer nivel de seguridad de este sistema.

Durante un tiempo los Hackers se vieron frenados y nada pudieron hacer. El algoritmo era complejo y utilizaba una palabra de control de varias decenas de bits. Y lo que era peor, estos códigos no eran repetitivos. Puesto que se sabía que las tarjetas de acceso se basaban en el estándar de comunicación ISO 7816, se podían leer las comunicaciones de dicha tarjeta con el descodificador a través de una interface programada. Pero los comandos que iban y venían, en una y otra dirección variaban de forma constante. Sin embargo se constataba que un sistema no podía trabajar con

claves aleatorias. De hecho ningún sistema puede hacerlo así. Eso era una esperanza. Rider Shamir fue el encargado de crear el algoritmo nuevo que pondría en jaque a los piratas. El código se denominaba RSA y se creía mas seguro que el estándar americano DES, un algoritmo que se permutaba hasta 16 veces.

Durante un tiempo Murdow durmió tranquilo hasta que un buen día a un estudiante de informática se le ocurrió preguntar a su profesor como funcionaba el sistema de codificación del canal SKY. El profesor le respondió que no lo sabía exactamente, que sentía cierta curiosidad por el sistema y que le había llamado especialmente la atención el hecho de emplear una tarjeta inteligente.

El alumno se encogió de hombros y animo al profesor a que estudiara la forma de revelar el algoritmo del sistema. Entonces el profesor le preguntó cual era la razón para que le invitara a hacerlo. Si la complejidad del sistema u otra razón. Entusiasmado el alumno le contestó que le agradaría ver la serie de Star Trek que emitía dicho canal de pago. El profesor se encogió de hombros y le invitó al alumno a que se sentase.

Durante un tiempo las palabras del alumno le rondaron por la cabeza como una obsesión incontrolada. El profesor había desarrollado un interfaz con un pequeño programa para estudiar y leer lo que se avenía entre la tarjeta y el descodificador con la intención de enseñar a sus alumnos como funcionaba el protocolo ISO 7816. Ademas de los códigos de control comunes de este protocolo habían otros códigos hexadecimales que variaban constantemente, pero pronto cayó en la cuenta que ciertos códigos se repetían esporádicamente y que si seguía con detenimiento la cadena de datos, estos se repetían asiduamente a lo largo de un periodo.

Un mes después dio con la clave y tuvo a punto la primera tarjeta electrónica basada en un micropocesador de Arizona Chip, un PIC 1654. El nivel de seguridad del sistema se denominaba nivel 6 y el profesor se sentía satisfecho de haber conseguido abrir el sistema con cierta facilidad.

Al día siguiente de crear la tarjeta se la regaló al alumno invitándole a que viera Star Trek y de paso sirvió como modelo de estudio para toda la clase. Y así fue cómo empezó una feroz batalla de códigos entre New Datacom, la creadora de códigos de SKY y los piratas.

Como era de esperar dicha tarjeta cayó en manos de otros piratas y pronto los códigos y tablas se difundieron con rapidez. Había quien había visto con buenos ojos un negocio fructífero y pronto miles de tarjetas clónicas invadieron Europa.

Semanas después New Datacom cambio el código 6 al código o nivel 7. Pero pocas eran las variaciones hechas en el sistema, ya que el profesor dio de nuevo con la clave una semana después. Y creo las tablas.

Estas tablas permitían cambiar el numero secreto de la tarjeta, por tanto un mismo algoritmo adoptaba formas diferentes en cualquier momento. Durante mas de un año

New Datacom cambiaba esta clave, pero un cambio por esta tabla reiniciaba de nuevo las tarjetas piratas.

Y es que un algoritmo puede sufrir alteraciones con solo cambiar un octeto y eso es lo que hacían, pero el algoritmo era el mismo, sólo se cambiaba un par de códigos y estos códigos estaban disponibles en una tabla ya preparada. Con ayuda de un reprogramador era posible activar de nuevo cada tarjeta después de cada cambio de código. Entonces fue cuando New Datacom introdujo una novedad en sus códigos. Cada tarjeta poseía un numero de identificación y se podía modificar dicho numero por vía aire y a través de Software. Ademas los PIC podían ser modificados externamente y pronto se supo que todos los PIC ya tenían un número clave de serie. Los ingenieros de New Datacom adquirieron algunas de estas tarjetas piratas en el mercado negro y las estudiaron con detenimiento y pronto encontraron el fallo.

La respuesta fue modificar el Software de la tarjeta para que respondiera de otra forma. De esta forma los piratas tenían que modificar sus tarjetas si querían seguir vendiendo. una vez que se logro el proceso, se introducía la contramedida electrónica ECM, junto con los códigos secretos y se bloqueaban las tarjetas piratas con esta medida electrónica. paradójicamente cayeron todas las tarjetas y el código ECM se había convertido en una forma más de anular estas tarjetas sin tener que cambiar los códigos de forma continuada.

Ya que había que tener en cuenta que las tarjetas oficiales tenían que seguir funcionando sin tener cortes en su funcionamiento. Pero el protocolo 7816 permitía ciertas modificaciones de Software y seguir funcionando.

Paralelamente los piratas y como en todo cada uno tenia su misma versión de la misma idea. Abrir y engañar al sistema más fuerte anunciado hasta el momento. Así otra de las formas de hacerlo era modificando el Software del programa que albergaba el microprocesador de control de comunicación con la tarjeta. Se escogía la instrucción que daba autoridad para habilitar otro chip especifico encargado del desembrollamiento de la señal de vídeo y se anulaba o se simulaba independientemente de la respuesta de la tarjeta de acceso oficial. Para ello se cambiaba dicho microprocesador por otro que estaba trucado. A este método lo bautizaron con el nombre de Kentuky fried chip y duró mas o menos un año hasta que los ingenieros de New Datacom modificaron el programa de dicho chip, pero eso es algo que solo son rumores ya que se cree que todavía hoy funciona. Lo único engorroso que tiene es que hace falta modificar el descodificador y no siempre es posible hacerlo, ya que un usuario puede estar a miles de kilómetros del taller.

Por ello se optaba mas libremente por la adquisición de una tarjeta clónica. Era menos complicado y ademas se podía enviar por correo. El único inconveniente es que debía reprogramarse cada cierto tiempo.

Pero pronto pasaron a la versión 08 y 09 y fue cuando hubo un gran parón y

surgieron nuevas ideas para hacer un Hack definitivo que nunca fue, del sistema más emblemático de todos.

Así nació el Phoenix Hack.

El resurgir del ave, así se rebautizó la nueva promesa que se mantuvo en secreto durante al menos dos meses de constantes pruebas en un laboratorio a las afueras de Hannofer. La nueva tarjeta pirata funcionaba pero presentaba ciertos problemas cuando llevaba algún tiempo insertada en el descodificador. En un principio la existencia de esta tarjeta sólo era un rumor, pero los medios de información ya se habían hecho eco de ello y publicaban extensos artículos rememorando la tarjeta pirata versión 07 que había sido presentada en una feria de Francfort en el año 94, por un grupo de ingenieros. Pero nada mas lejos de la realidad. La vieja tarjeta versión 07 denominada Hipercrypt en aquel momento se había presentado junto al Kentuky Fried chip.

Y volviendo a los nuevos Hacks de la versión 08 y 09 cabe destacar que se apuntaron al éxito numerosas empresas autorizándose el dominio del mismo, pero lo cierto es que estas tarjetas siempre han sido creadas por una misma persona, al contrario de lo que se pretende hacer creer en un mundo donde se falsean los datos.

El profesor de informática, cuyo apodo es Zap, tenía en jaque a todo un poderoso centro de investigación de seguridad como New Datacom. Su nueva tarjeta basada en dos poderosos chip PIC 1684 estaba lista para funcionar.

Paralelamente al Phoenix otras empresas seguían fabricando «cartones electrónicos» como se les denominaban en aquellos gloriosos días. Ya que no todos los canales que estaban codificados con el sistema de codificación de Videocrypt no trabajaban con el mismo código, todavía existían canales que funcionaban bajo el código 07 y el profesor ZAP vendió sus códigos con el nombre de SEASON 7 (este programa fue actualizándose hasta alcanzar la versión Season 13). El programa en un principio se pagaba como si se trataran de lingotes de oro y así fue como varias empresas fabricaban sus propias tarjetas piratas. Empresas tales como Megatek e Hi - Tech consiguieron colocar en el mercado miles de estas tarjetas con códigos 07.

Mas tarde cuando los códigos cambiaron a 08 y 09, estas empresas habían negociado con el profesor ZAP y tenían lista sus propias versiones. Pero el profesor ZAP era cauto y les advirtió que no lanzaran todavía el producto ya que según el todavía existía un fallo en los códigos a pesar de que funcionaba bien.

Las nuevas tarjetas se lanzaron al mercado y cayeron fulminadas unas dos semanas después. Por ello la confianza degeneró en miedo y ya nadie compraba tarjetas piratas. New Datacom había pasado decididamente al código 09.

Mientras el código 09 maduraba en el laboratorio del profesor ZAP, otras empresas lanzaron otros Hacks basados en tarjetas oficiales. Esto inspiraría mas confianza al comprador. El sistema se basaba en bloquear los códigos ECM de

borrado de tarjeta mediante una interface electrónica entre el descodificador y la tarjeta legal u oficial. A este circuito se le bautizo con el nombre de Bloquers y aunque surgieron varios de ellos, (El mas destacado fue la Sunbloquer de Hungría por ser la mas eficaz) uno de ellos recibió el nombre de Lázaro. Como una alevosía a la resucitación de los piratas.

Los bloquers permitían activar tarjetas caducadas y ademas impedían que estas se desactivaran desde el centro de control de abonados. El sistema funcionó bien hasta que los ingenieros de New Datacom contraatacaron con nuevos códigos ECM «control de medida electrónica» para desactivar definitivamente las tarjetas legales. el sistema se basaba en una instrucción secreta que fundía el fusible de lectura de la tarjeta chip. Y así fue como se impuso de nuevo la nueva tarjeta pirata versión 09, después del desastre de la desactivación de mas de 100 000 bloquers en un solo día.

La nueva versión 09 también poseía códigos variables y tablas. El algoritmo seguía basándose en la norma RSA y solo se había complicado en un octeto mas de instrucción. Ademas existían códigos que no actuaban sobre el encriptado o el algoritmo, pero estaban hay y servían para algo, pero no se sabía para que exactamente. Mientras tanto el código 07 se servia en un servidor de Internet y uno podía fabricarse una interface que se conectaba al ordenador y el descodificador y podía ver aquellos canales de videocrypt que conservaban los códigos 07. Cuando había un cambio de claves, solo tenias que probar con varios números desde el ordenador y rápidamente se activaba la tarjeta. Probablemente el sistema de Videocrypt haya sido el sistema mas pirateado del mundo y el que más cambios ha conocido. y aun hoy a estas fechas en las que se escribe este libro sigue la dura lucha entre los piratas y New Datacom.

Durante varias semanas la nueva tarjeta del profesor ZAP funcionó correctamente, pero eso solo era una maniobra de New Datacom que tenía preparada una coartada. La nueva tarjeta oficial tenía mucha mas memoria ROM interna y mucha más memoria RAM. Lo cual en un principio desconcertó al profesor ZAP. Pero NEW les tenía preparado una sorpresa.

Como era habitual, los cambios de códigos se efectuaban siempre el día de navidad y la fecha estaba próxima. Cuando por fin llegó el día todas las tarjetas piratas reaccionaron de forma extraña. Solo descodificaban por momentos y presentaban extraños mensajes en la pantalla del televisor. Ya que estas tarjetas no poseían fusibles internos que desactivar y eran inmunes a los ECM, NEW decidió que la nueva versión debía ser cuasi-aleatoria y que debía permitir modificar los códigos cada 48 horas. Y eso fue lo que sucedió.

Las tarjetas piratas se volvieron locas y de nuevo la incertidumbre reino en este peculiar universo. Pero el profesor ZAP también tenía su coartada.

Una nueva tarjeta denominada Card Mate estaba en proceso de creación. Ahora se

aumentaría la memoria interna y ademas esta nueva tarjeta seria reprogramable a través de un teclado al tacto. Y seria tan sencillo hacerlo como introducir un número de teléfono.

La nueva Card Mate estaba basada en un potente chip de Dallas DS 5002 y ademas estaba preparada para nuevos códigos futuros y así sucedió.

Un año después New Datacom decidió cambiar a la versión OA. Ridher Shamir cobro una importante suma por modificar su algoritmo RSA de seguridad, pero el capitán ZAP le estaba esperando.

Cuando hubo el cambio de la versión 09 a la versión OA, solo se hubo que reprogramar las tarjetas Card Mate. Y fue así como el capitán ZAP ganó la batalla.

3.6. Otros casos de Hacking no menos importantes

Filmnet, un canal de cine las 24 horas, fue uno de los primeros canales de televisión vía Satélite que decidió codificar su señal allá por el año 1986. Concretamente el 1 de Septiembre, con un sistema de cifrado basado en tecnología analógica. Durante los siguientes cinco años conoció hasta 6 variaciones del sistema.

La primera versión era extremadamente sencilla y fácil de clonar, por lo que fue uno de los primeros sistemas en ser pirateado con éxito, después del sistema de codificación de SKY en ese mismo año. Ambos canales empleaban codificaciones similares basados en las mismas bases y fundamentos. Pero el OAK ORION que así se llamaba el sistema de codificación de SKY antes de adoptar el sistema de Videocrypt, no conoció modificación alguna a pesar de estar clonado con éxito.

El 23 de marzo de 1987, se decide cambiar algunas secuencias en la codificación del sistema de Filmnet, denominado SATPAC, con la esperanza de dejar fuera de servicio los descodificadores piratas. Sin embargo el intento fue en vano, ya que un simple modificación volvía a renacer el descodificador pirata.

El 24 de Diciembre de 1989 Filmnet cambia de nuevo sus códigos y es que parece que la fecha de navidad es siempre la propicia para estos cambios, como si de un regalo de navidad para los piratas se tratara. Pero de nuevo el intento era fallido, puesto que se volvieron a cambiar los códigos nuevamente el 11 de mayo de 1990, de nuevo en diciembre de 1990, en enero de 1991 y en marzo de ese mismo año.

Hi-Tech, con sede en Inglaterra, era la empresa encargada de fabricar

masivamente los descodificadores piratas y algunos medios de publicaciones electrónicas, publicaron sus propios descodificadores.

Ese mismo año Filmnet introdujo una codificación del audio digital y durante unos años los piratas vieron frenados sus deseos, pero la llegada de potentes chips en el sector de la electrónica de consumo, hicieron posible la apertura del sistema.

Pero quizás el caso mas sonado fue y será la masiva clonación del sistema adoptado por Canal Plus Francia y su sistema de codificación DISCRET 1, que mas tarde se convertiría en la versión 12. De este sistema se fabricaron mas de un millón de descodificadores piratas y de nuevo la empresa inglesa Hi-Tech estaba detrás de todo esto.

Este sistema también fue objeto de estudio y publicado en las revistas de electrónica más prestigiosas del momento. El sistema de codificación analógica, también permitía variaciones de códigos, pero los Hackers siempre estaban atentos y ya habían predicho dichos cambios con anterioridad.

Finalmente Canal Plus adoptó un sistema digital más seguro, que puso fin a la piratería más grande jamás conocida.

Un caso parecido sucedió con el sistema SAVE de la BBC, que se estaba empleando en un canal hardcore. En esta ocasión no se empleaban códigos y era fácil de clonar y es que durante un tiempo en el que sólo, reinaban los sistemas de codificación analógicos, la polémica estaba servida.

Con todo esto quiero hacer especial hincapié en lo referente a seguridad. Es un factor muy importante, pero que no siempre se consigue. Volviendo a los códigos RC5, IC2 o el protocolo ISO 7816, cabe destacar que si estos códigos hubiesen sido absolutamente secretos en vez de públicos, probablemente hoy día estarían disponibles en algunas publicaciones y en algún servidor de Internet.

Con lo cual concluyo que estamos ante un factor importante pero que no siempre se logra el objetivo. Ya que por el momento sigue la batalla por el dominio y la seguridad.

3.7. El Crack del código CSS

La prensa se ha hecho eco, y ha divulgado este Crack como uno de los más importantes ocurridos en los últimos años. Tal ha sido la envergadura del hecho, que

los principales Fabricantes de electrónica y Productores de Hollywood, han demandado al grupo de Hackers y a todos los que de alguna manera, tengan que ver con la distribución del Programa DeCSS.

La debilidad del algoritmo de encriptación de los discos DVD, «40 Bits» ha permitido a un grupo de Hackers Noruego «MoRE, Masters of Reverse Engineering», entre los que destaca Jon Johansen, un estudiante de 15 años, a descubrir que en su ordenador, el sistema de protección del DVD podía «romperse» con un programa pequeño y relativamente simple que creó en unas pocas horas.

El DeCSS permite volcar el contenido de un DVD al disco duro de un ordenador y reproducir la película con calidad perfecta. También, este pequeño programa permite crear un duplicado desprotegido del contenido DVD en un disco virgen por medio de una Grabadora, con la misma facilidad con la que hacemos una copia de archivos. A las pocas semanas de aparecer DeCSS en la ReD, se decide retrasar el lanzamiento del DVD-audio, dado que se cree conveniente introducir un nuevo nivel de protección mucho mas potente, que permita al mismo tiempo dejar obsoleto al DeCSS. Se presenta así, CSS2, un algoritmo más complejo que el endeble CSS «Content Scrambling Systems», sin embargo creemos fervientemente que CSS2 dejará de ser seguro muy pronto.

A la pregunta, de como habían conseguido obtener la clave de cifrado del DVD, los Hackers respondieron, que gracias a la debilidad del algoritmo empleado para el cifrado del disco DVD, 40 bits en una clave única, que por la estructura del propio algoritmo, bien podría ser una clave de 20 o 25 Bits fácilmente «desmenuzada» por un ataque directo de fuerza bruta. Sin embargo, no fue la fuerza bruta, la que les abrió el camino a descubrir la verdadera clave, sino un error de protección de la clave de apertura del Software Reproductor XingDVD, realizado por una filial de la conocida RealNetworks.

Cada DVD se cifra con una clave aleatoria de 40 bits. Esta clave de sesión se cifra a su vez con la clave de apertura de cada fabricante de Hardware o Software, lo que nos permite determinar que cada DVD, contiene la clave de sesión de cada Fabricante y como resultado da, que cada DVD posee cientos de claves para iniciar la lectura del disco. Cuando un Reproductor va a leer el disco, lee primero la clave de sesión cifrada con su clave de apertura, la descifra «empleando para ello su clave de apertura» y luego la utiliza para reproducir el resto del contenido del DVD.

Los Hackers localizaron gracias al error del Reproductor XingDVD, unas 180 claves en un disco DVD. Una vez obtenida la clave de apertura, se tiene acceso a cualquier DVD y lo que es peor, si se emplea un ataque por fuerza bruta, se obtienen, ademas, todas las claves que el DVD contiene. Dicha «fuerza bruta» es tan simple como obtener la clave de sesión del XingDVD y seguidamente aplicar claves aleatorias en una EXOR hasta obtener las claves buenas. Para realizar esto, el grupo

de Hackers, creó un programa exclusivo para esta tarea, lo que le llevo a descubrir las 180 claves en tan sólo unas pocas horas de cálculo.

En la actualidad estudiantes del prestigioso MIT a desarrollado un programa escrito con sólo 7 líneas de código, capaz de descrifrar el anticopiado del DVD.

3.8. El Crack del código regional

El primer Crack del código regional, se debe a la sucesión de los Chips que permitían cargar discos piratas, en las consolas Playstation y por lo tanto, responde a la categoría de Crack por Hardware. El famoso Microntrolador 508 de Microchip, se empleaba de nuevo para «engañar» la secuencia de Boot o de arranque del disco. Tal como sucedía en las consolas de Playstation, la secuencia de arranque del disco, parte que contiene el código regional, era sustituido por varios ceros a fin de indicar al Reproductor de la existencia de un disco universal.

Este Crack es un tanto difícil de llevar a cabo, ya que conlleva el abrir el reproductor DVD, que en cualquier caso pierde la garantía en el momento de abrirlo. Sin embargo en la ReD existen unas muy buenas Guías de cómo llevar a cabo la «operación» con cierto éxito. Según los Crackers, el llevar a cabo la implantación de este Chip en el Reproductor DVD, no es tanto cómo una tarea de chinos, ya que, aseguran desde sus páginas Web, que los fabricantes han facilitado, en parte la tarea, ya que sus Reproductores cuentan con un diseño flexible, que les permite modificar el código de lectura regional, a fin de poder distribuir dichos Reproductores en cualquier parte del mundo.

Esta Flexibilidad, se basa en la disposición de Jumpers, pistas marcadas o chips con pines que se pueden soltar del circuito impreso. Estos detalles, permiten al servicio técnico, adaptar sus Reproductores al código regional deseado, punto débil que los Crackers han aprovechado para sacar a la luz los Firmwares, una nueva moda de modificar Reproductores DVD con y sin el Chip 508.

Por otro lado, cada día, son más los lectores de discos y las tarjetas Hardware, que permiten reproducir contenidos DVD en el Ordenador. Esto ha generado también, la existencia de un Crack por Software, que en muchos casos se basa en renombrar un fichero DLL y en otros casos, basta con parchearlos.

3.9. El Crack de Macrovision primera parte

En Octubre de 1988, la prestigiosa revista de electrónica Elektor, publicaba en sus páginas un «Interval Blanking» algo así como un borrador de señales blancas. En realidad se trataba, del primer decoder, capaz de borrar la señal de anticopia de Macrovision. Se trataba de un circuito capaz de crear una ventana de captura, en la cual introducía nuevos niveles de negro capaces de sustituir los niveles positivos de la señal de anticopia de Macrovision.

En realidad esto es un poco difícil de entender, sobre todo si no conocemos como esta compuesta una señal de vídeo. Sin embargo creemos que las siguientes líneas, os aclararan las ideas. El decoder propuesto por elektor electronics, se basaba en un extractor de sincronismos, varios conmutadores digitales y un par de monoestables.

La idea era la de extraer los sincronismos verticales de la señal de vídeo. Dichos sincronismos, son los que indican cuando empieza un campo de vídeo. Esta señal, denominada, impulso Vertical se encargaba de disparar un primer monoestable, el cual mostraba un nivel de disparo, pasado un tiempo. De esta forma sé conseguía crear una espera o inicio de la ventana de captura, unas cuantas líneas mas tarde que el impulso Vertical de vídeo.

Un segundo monoestable, se encargaba de crear una ventana de captura, lo que permitía, de alguna manera, «atrapar» los pulsos de anticopiado dentro de una ventana virtual, la cual era reflejada en un par de conmutadores electrónicos. De esta forma, en el momento que existía una señal de anticopia de vídeo, ésta, se bloqueaba en la entrada de uno de los microinterruptores, y en su lugar, se aplicaba un nivel de negro estándar, a fin de que los circuitos CAG del videograbador no detectase ninguna anomalía en la señal de vídeo. Tras esto, justo cuando la señal de anticopia desaparece, los micro- interruptores, vuelven a su estado inicial, dejando pasar el resto de la señal de video.

Sin embargo a pesar del interés de la Multinacional Macrovision, de ganar una demanda que había cursado contra la revista elektor, el decoder no funcionaba todo lo bien que se deseaba. En 1993 cuando el circuito se publica en España, «En la versión española de dicha revista» un curioso de la electrónica de tan solo 23 años, que responde al apodo de OverrideSidek, diseña el que será, el decoder de Macrovision más rentable de los últimos 6 años.

El circuito se publica en una prestigiosa revista de electrónica llamada Resistor, un año mas tarde y durante los primeros dos meses, se hacen unos 3.000 pedidos del decoder.

Aunque Internet ya existía, al menos, en nuestro País, no era particularmente empleado y por supuesto, sé desconocía de la existencia de páginas en la ReD con contenidos explícitos para decodificar Macrovision. Sin embargo, la ola de decoders

no sé hacia esperar, ya que tres años más tarde, en 1997, comienzan a proliferar las páginas que de alguna u otra manera, hablan de como decodificar el sistema de anticopia de Macrovision.

Sin embargo, no es hasta finales de 1999 y tras surgir en el mercado, toda una legion de reproductores DVD para PC y Sintonizadoras de Televisión, cuando el Crack de Macrovision, conoce una nueva línea a seguir. Ahora, el Crack de Macrovision se basa en el empleo de Software, programas capaces de desabilitar la función de Macrovision.

Algunos programas parchean un fichero determinado y otros, mas sofisticados, manipulan los Drivers de las tarjetas reproductoras DVD y sintonizadoras de vídeo con salida de televisión, también denominadas TVOut.

3.10. El Crack de C+, Discret y Nagravision

El Crack más importante de todos es, quizás es el de Canal Plus, quizás en parte, porque es el primer canal de pago fuera de las fronteras de Sky, quizás por que era él mas esperado entre la comunidad Underground. Jesús de Polanco es el segundo hombre más poderoso en el sector de las telecomunicaciones, en clara competencia con Rupert Murdock. Su canal de pago, Canal Plus es bien recibido con una importante acogida traducida en miles de abonados nuevos cada semana.

En Noviembre de 1984, Canal Plus inicia sus emisiones empleando el sistema de Encriptación Discret 1 de Philips, dicho sistema es proclamado como él más vulnerable del mundo, en la comunidad Hacker. Es el primer canal de pago en Francia y por lo tanto, el sistema de cifrado más débil del momento, algo bien recibido por la comunidad Hacker. En Diciembre de ese mismo año, esto es, un mes mas tarde, la revista francesa de electrónica Radio Plans, publica un articulo en el cual, se muestra como construir un decodificador pirata para ver Canal Plus. El diseño que la revista propone no infringe la Patente, pero incita a la fabricación de estos decoders. En tan solo unas semanas, casi todo el mundo en Francia disponía de una fotocopia de este articulo.

Esto permite la masiva clonación del sistema adoptado por Canal Plus Francia y su sistema de codificación DISCRET 1, que más tarde se convertiría en la versión 12. De este sistema se fabricaron mas de un millón de descodificadores piratas y de

nuevo la empresa inglesa Hi-Tech estaba detrás de todo esto.

Este sistema también fue objeto de estudio en 1987, y publicado en las revistas de electrónica más prestigiosas del momento, ademas de la citada Radio Plans. El sistema de codificación analógica, también permitía variaciones de códigos, pero los Hackers mas avispados, ya estaban en ello y ya habían predecido dichos cambios con anterioridad. Discret así, conoce una vida de tan solo 6 años, ya que finaliza en 1990, año en la que surge un nuevo nivel en Discret, estamos hablando de Discret 12. El nuevo nivel, se basa en los mismos métodos que la versión Discret 1, pero introduce la tecnología digital y la posibilidad de cambiar los códigos cada mes o más a menudo. Los Hackers sufren un golpe leve, ya que ese mismo año comienzan a fabricar un nuevo decoder, también digital, que permite adaptarse a los nuevos códigos con solo introducir una clave mediante teclado.

Finalmente Canal Plus adopta un sistema digital más seguro, que puso fin a la piratería más grande jamás conocida. Paradójicamente, el nuevo método de cifrado digital, en el que apostaba fuerte C+, fue estrenado en nuestro país hacia el año 1994, la nueva arma de guerra se llamaba Nagravision, y estaba avalada por Andre Kudelski, uno de los mejores Ingenieros de Europa en métodos de embrollado de audio.

Nagra Kudelski, la empresa Suiza, lanza su sistema de codificación también denominado Syster G1, a mediados de 1991, manteniendo en jaque a la elite Hacker durante mas de cinco años. Finalmente, en 1996, después de obtener información de un Cracker Español sobre Nagravision, en Francia, a menos de un año de haber estrenado Syster en Canal Plus Francia, surgen los primeros decodificadores piratas en Hardware.

Internet ya esta implantado con fuerza en Europa y los esquemas y ficheros de este decoder, se cuelgan en una BBS a disposición de todos, lo que facilita la fabricación en serie de este decoder, por los menos escrupulosos del momento. El decoder solo funciona para la versión SECAM y en España, la comunidad Hacker apenas conoce la existencia de este decoder, en nuestro país solo existen los rumores. Empleando componentes de gran calidad, el decoder pirata comienza a venderse de forma alegre en el mercado negro, lo que lleva a dar la alarma entre los directivos de Canal Plus. En solo unos meses la gendarme francesa realiza la mayor redada del momento, deteniendo a los responsables de varias empresas que se dedicaban a fabricar estos decoders al por mayor.

La noticia salta a la prensa y en España, la comunidad Hacker se asombra de la existencia de este Decoder tan perseguido en nuestro País, que siempre había sido un mero rumor, pero ya es demasiado tarde, las paginas que albergaban los esquemas y ficheros para programar los diferentes Chips del decoder, ya han sido cerradas y nadie sabe quien puede tener una copia.

Ese mismo año Markus Khun, el mayor «investigador» de Europa, «creador de las tarjetas electrónicas para ver Sky gratis» crea un programa capaz de descodificar el sistema de Nagravision, a través de un ordenador. La única pega, es que solo funcionaba en una Sparc 40 y para ello debías invertir una cantidad importante de dinero, esta fue, sin embargo el principio de la descodificación PCTV que actualmente conocemos.

A finales de 1998, alguien coloca en la ReD un Software capaz de decodificar parte de la señal de Nagravision, se llama NagraDec83 y es capaz de desencriptar u ordenar, una imagen embrollada en Nagravision, en un ordenador que posea una capturadora de Televisión. Las capturadoras de televisión son ya una realidad y pronto aparecen mas y más programas, capaces de descodificar ya en tiempo real, una señal embrollada con el sistema Nagravision, aunque con mala calidad de imagen.

Los programadores Alemanes, parecen tener ganada la carrera con su Pubs, Un Software rápido y potente, capaz de descodificar de forma perfecta, la señal de Canal Plus. Ahora los programadores salen de todas partes, y cada uno de ellos, aporta su creación, siempre basada en el Chip Universal BT 848 / 878, que emplean el 90 % de las Capturadoras de Televisión.

A fecha de hoy, cualquier Software de este tipo, es capaz, ademas de decodificar Canal Plus, cualquier señal codificada en VideoCrypt, Discret o Cablecrypt. Lo atractivo del asunto, es que todo el Software es gratuito.

3.11. El Crack de Save y la venta de Enigma

Hi-Tec estaba detrás de todo una vez más. Un caso parecido al Crack de Discret 1, sucedió con el sistema SAVE de la BBC, que se estaba empleando en un canal hardcore. En esta ocasión no se empleaban códigos y era fácil de clonar y es que durante un tiempo en el que solo, reinaban los sistemas de codificación analógicos, la polémica estaba servida.

Hi-Tec era la empresa que fabricaba el 90 % de los descodificadores piratas en Europa y sucedió que llego a fabricar mas de 3 millones de unidades para el sistema SAVE. La BBC demando a Hi-Tec por esto, sin embargo el Canal Hardcore no hizo lo mismo. Los directivos del canal porno decidieron, que era mejor contratar los servicios del Hacker, antes que arremeter contra él, ya que según ellos, estaban

comenzando con un canal de televisión vía Satélite en un momento en la que todo eran problemas.

La gente preferiría siempre adquirir un decoder pirata para ver películas Porno, antes que decirle a la mujer, si estaba de acuerdo en abonarse a dicho canal. Probablemente, a pesar de estar viviendo en Holanda o Alemania, países de cierto liberalismo, esto terminaría con una tremenda discusión familiar.

RedHot, que así se llamaba el canal de televisión porno hablo con el Hacker, bueno, en realidad quien hablo con el Hacker fue un directivo de este canal. Esto fue en Barcelona, durante una importante feria del Satélite. Josep Borrell iba a inaugurarla ese día, y el que aquí escribe acababa de sacar a la luz un libro sobre Sistemas de Codificación. El primer libro de este tema, en español.

Dos horas antes de que la policía de Seguridad «los cabezas de turco del ministro de comunicaciones» irrumpiera en la sala principal, no sé que tipo de arma en mano, con la intención de comprobar que todo estaba bien para la entrada del señor Borrell, tuvo una importante reunión entre un directivo del Canal y el Hacker.

Una tía de enormes tetas, mostraba una estúpida sonrisa en su cara salvajemente maquillada, mientras su cuerpo de gigantescas curvas se desparramaba sobre una silla que estaba situada casi a la altura del mostrador, algo que permitía mostrar algo más que la «cana del pecho». El Hacker estaba detrás de esta impresionante mujer, sentado en una silla que no podía ver desde donde yo estaba. Ahora la mujer de las tetas enormes me guiñó un ojo. Al otro extremo de la mesa, un hombre canoso, recio y con un despliegue de papeles sobre la mesa, acababa de cerrar un maletín negro, con la pasmosa habilidad de alguien que cree que la maleta va a estallar en mil pedazos si la cierra de golpe. El dedo índice de la mano derecha de la mujer, estaba formando un gancho. Vete a la mierda pensé, pero le dedique una forzada sonrisa, su enorme cabezón me estaba impidiendo ver el rostro de sorpresa del Hacker.

La mujer se puso pesada y me dijo algo en no sé que idioma, seguramente me estaba llamando para darme la lata de lo bueno que era el canal hardcore. Era un reclamo de nuevos abonados al canal que veía aguas. La gente ponía cara de sorpresa al pasar delante de ella. Mas adelante descubrí que aquella mujer de voluptuosas tetas era una actriz Porno que había hecho no sé cuantas películas en su corta carrera de actriz hardcore. El Hacker estaba ahora firmando un documento. Media hora más tarde, me entere por el mismo, que es lo que había firmado.

Campbell, que prefiere permanecer en el anonimato, «su nombre real no es Campbell, así es como lo llamo yo» pertenecía a la factoría Hi-Tec y era uno de los mejores hombres de la empresa. En realidad era quien había conseguido descifrar el audio Digital de Filmnet, Clonar una tarjeta del sistema D2-Mac o de copiar una tarjeta SmartCard del grupo Sky.

Los hombres de RedHot se habían enterado de que Carey andaba buscando

alguien que se interesara por su sistema de Codificación Enigma. Un sistema similar al de Videocrypt, capaz de descodificar los canales de Sky si se empleaba una tarjeta original. Campbell le habló de precios al gran directivo y este aceptó.

Pocos meses después el canal ReDHot que emitía a través de Eutelsat, cambiaba la codificación SAVE, por Enigma y por supuesto, nadie sacó el Crack para este sistema. Seis meses mas tarde, el canal porno desapareció y los descodificadores de Enigma se vendieron para descodificar otro canal Hardcore, esta vez llamado Adult Channel y que estaba codificado con Videocrypt.

3.12. El Crack de Macrovision segunda parte

En Octubre de 1988 la revista Elektor publica en sus páginas lo que ellos denominan «Blanking Interval» se trata de un eliminador del sistema de anticopia de Macrovision. La idea es buena, sin embargo el circuito no termina de funcionar todo lo bien que se desea, no obstante el gigante de Sunnyvale, Macrovision hace una demanda formal contra Elektor, en la que alega, que la revista publica contenidos que dañan la Patente de Macrovision.

La CBS es la primera productora que incluye este sistema de anticopia en uno de sus títulos, concretamente se trata de *Back to the Future,* de Robert Zemekis. Esto fue en 1983, pero cinco años mas tarde la cinta es recuperada y estudiada. Absurdo dijeron algunos en su momento, porque no elegir una película del momento?.

El Hacker quería comprobar que todo seguía igual, pero no fue así. El código de Anticopia había cambiado desde una cinta a otra. Era de suponer, ya que el código de Anticopia, de alguna manera, afectaba negativamente en la calidad del video. Por esa misma razón los ingenieros de Macrovision introducen nuevas mejoras en el código cada pocos meses.

En 1990 se presenta un segundo decoder de Macrovision, en la comunidad Hacker. La nueva versión es mucho más estable, pero por alguna razón las revistas especializadas en Electrónica no se hacen eco de el. En 1994, OverrideSidek crea el primer decoder de Macrovision con solo tres Chips y lo vende a una prestigiosa revista de electrónica en nuestro país. El decoder es difícil de ajustar, pero funciona a la perfección, sin embargo el hecho de que el decoder necesitara algunos ajustes para la puesta en marcha, hace que el técnico de la revista se saque de la manga una nueva

revisión de este decoder de Macrovision.

Esta vez se añadía una PAL programable. OverrideSidek contraataca en 1998 con un nuevo decoder mucho más avanzado. OverrideSidek introduce un control de CAG, esto seria la revolución, ya que su decoder es capaz de limpiar perfectamente cualquier nivel del sistema de Anticopia de Macrovision.

Sin embargo el Crack de Macrovision no parece basarse solo en este tipo de decoders, capaces de limpiar la señal de anticopia, sino en una patente que OverrideSidek saca a la luz en 1995. OverrideSidek es el inventor de Enigma, un Generador de sistemas de anticopia para sistemas de vídeo.

El invento es simple, se trata de generar el mismo código que antes había eliminado. Un año mas tarde, OverrideSidek revisa su diseño y lo adapta a las grandes corporaciones, ya que Enigma estaba creado para el duplicado en pequeñas empresas que funcionaban con videograbadores normales. Para que Enigma funcionase con estos tipos de videograbadores, OverrideSidek crea un Crack letal, que permite anular el CAG de cualquier videograbador comercial, lo que supone el permitir copiar una película con Macrovision, sin necesidad de recurrir al decoder «interval Blanking».

Sin embargo, esto no parece molestar a los directivos de Macrovision. El problema surge después, cuando OverrideSidek crea EnigmaPlus, un sistema de Anticopia superior al de Macrovision. Era el año 1997 y un avispado empresario de Santander logra colocar Enigma y enigma Plus en los principales bancos de duplicado del país. A partir de ese momento el código enigma ya forma parte de las mejores películas del momento. Tri pictures, Fox o Warner son algunas de las productoras que reciben el nuevo código español.

El empresario de Santander se frota las manos, y cambia la estrategia comercial del producto, en lugar de venderlo, decide alquilar enigma a las productoras y bancos de duplicado. Macrovision cobra unas 5 pesetas por cada película que contiene el código Antitaping, el empresario de Santander ofrece un royalty de 3 pesetas por película. Esto es un negocio que se teje a la sombra de OverrideSidek, algo que no le gusta nada y que termina en la ruptura de la relación, ya que el empresario de Santander había recibido ya algunas entregas de dinero a espaldas de OverrideSidek.

Pero el mundo es pequeño y la afición de analizar cintas de video que tiene OverrideSidek, le lleva a descubrir que Enigma esta incluido en algunas cintas de video y por supuesto a descubrir la trama. Estamos en 1999 y uno de los técnicos de la planta uplicadora de Walt Disney envía 10 cintas de video con el código Enigma Plus a Estados Unidos. OverrideSidek sabe de ello, pero no le presta especial importancia. Dos meses después OverrideSidek recibe una llamada de Mattew, responsable de Macrovision en Europa. La conversación dura cerca de dos horas y ambos hombres llegan a un acuerdo. OverrideSidek les confía su tecnología a

Macrovision y para ello envía unas cintas de video con el código, fotocopia de la patente y algunos esquemas, a Sunnyvale.

En vísperas de Navidades de ese mismo año, OverrideSidek recibe una carta certificada de un abogado de Macrovision. John Ryan, el fundador de Macrovision, desea que OverrideSidek deje de fabricar Enigma, algo que sorprende a OverrideSidek. Puestos al habla con el abogado de Macrovision, se saca a la conclusión que el empresario de Santander esta comercializando Enigma en la sombra, algo de lo que OverrideSidek ignora, pero que descubre por unos anuncios en una revista del sector.

Al momento de escribir estas líneas OverrideSidek me ha comentado que hace cerca de dos años que no fabrica Enigma, que el diseño es convertido en código fuente, esto es, que lo ofrece gratuitamente en la ReD, ya que dice tener un nuevo sistema de Anticopia mucho más avanzado y que pretende vender a Macrovision. El nuevo sistema de anticopia está diseñado para ser implantado en el DVD, Set-Top-Box e Internet. Bueno y quien sabe sí también en los ficheros MP3Pro o Divx.

3.13. El Crack de Irdeto digital y Nokia 9600

Cuando se habla de Irdeto y Nokia 9600 o 9800, se habla de dos Cracks diferentes. Pero es interesante hablar de ellos al mismo tiempo, ya que han marcado, los dos juntos, el inicio de una nueva etapa en el mundo del Crack en Televisión digital.

El receptor Nokia 9600 y 9800 después, han sido los receptores elegidos por los Hackers, para experimentar con la televisión digital, quizás por que son los más extendidos en Europa, al igual que Echostar lo es en Estados Unidos. El doctor OverFlow fue el primero en iniciar toda una línea de experimentos con este receptor digital. Su Software Edit DVB, telecargado desde un PC, podía modificar la información de la ROM de este receptor de Nokia.

Sin embargo este software solo permite modificar la estructura y presentación del Menú OSD del receptor, eso sí, permite controlar todos los aspectos del OSD en toda su extensión.

El Crack de Irdeto llega después, nadie sabe quien es el autor de este Crack, pero lo cierto es que el primer Crack de Irdeto permitía reactivar la tarjeta original de

Irdeto. Mas adelante la lista Underground engordaba por momentos. El siguiente crack de Irdeto se basaba en emular perfectamente esta tarjeta y una vez más, nadie sabia quien era el autor de este Crack.

3.14. El caso de BraKGroUp[1]

Básicamente este capítulo está basado en Cracks que a su vez, cuentan una historia de Hackers y Crackers. Necesitaríamos todo un libro para contar todo tipo de situaciones ocurridas en torno a los ordenadores y los sistemas de encriptado o anticopiado, que es donde, básicamente, se centran los Hackers. Con estas historias, quiero demostrar que el Hacking no es solo cuestión de ordenadores y de Internet, que el Hacking o mejor dicho el Cracking, es mas frecuente si cabe, fuera de la Red como se ha venido demostrando.

Las nuevas tecnologías como la televisión de pago, las videoconsolas o los teléfonos móviles, son capaces de mover los intereses de los Hackers, por estudiar estas tecnologías. Ademas de ser un reto mas, para los Crackers con menos escrúpulos, suponen una buena fuente de ingresos. Situación muy a menudo discutido en los foros. La siguiente historia gira en torno a BraKGroUp, quizás el primer grupo de investigación en serio que escribe un importante capítulo en nuestro país.

Denominado «Pongamosle» BraKGroUp, el nuevo grupo se forma en un momento en el que en nuestro País se empieza a tomar interés por un sistema de codificación implantado por la sociedad de Canal Plus. Dicho sistema, que emite C+, se denomina sistema de encriptado Nagravision. En Francia este sistema ya había sido Hackeado y en nuestro País estábamos a dos velas. De repente en Alemania, alguien escribe un programa de ordenador, capaz de desencriptar la señal de Nagravision, si esta se pasa a través de una capturadora. La fiebre se desencadena y se crea la primera página Underground sobre la televisión de pago. Es la página de «alguien que no pienso citar» y su emblema, BraKGroUp.

Movidos por la curiosidad, todos los internautas acuden a su página, en busca de grandes soluciones. Obviamente las encuentran, y no solo para experimentar con el sistema de Nagravision, sino para otros sistemas como Eurocrypt o Videocrypt. En estos momentos dicha página comienza a recibir una buena cantidad de visistas al dia y el autor a ingresar cierta cantidad de dinero por cada Internauta que visita su

página, gracias a los Banners publicitarios. En cierta manera, la pagina de BraKGroUp es una de las pioneras del momento y recopila todo lo que encuentra en la Red. Añadiendo cosas útiles y cosas inútiles, por causa de desconocimiento profundo sobre el tema.

Las plataformas digitales están a punto de hacer mella en los ciudadanos de todo el país y pronto se crea un vacío en la página de BraKGroUp. Faltan por abrir los sistemas de Seca Mediaguard y Nagra Digital. Esto motiva a que BraKGroUp haga un llamamiento a crear un gran grupo de trabajo, que más tarde se convertiría en un pequeño grupo de trabajo. En este grupo entran programadores de Microprocesadores y escritores de aplicaciones Windows o DOS.

Durante un tiempo mas o menos largo, el grupo no prospera y las preguntas a las incógnitas se vuelven gritos de desesperación, pero por fin y de forma paralela, en Francia e Italia rompen el sistema de Seca Mediaguard. Rápidamente el grupo de BraKGroUp es auxiliado con estos primeros pasos y un famoso manual que denominaré «BreaKcoDe «explica con todo lujo de detalles como funciona el sistema de Seca Mediaguard. BraKGroUp obviamente se queda atrás por falta de desconocimientos, sin embargo la troupe formada a su alrededor si conocen el nuevo lenguaje y se pone manos a la obra. El resultado, varias aplicaciones en DOS y Windows que permiten emular a la perfección el sistema de Seca Mediaguard.

Unos meses mas tarde, aparece otro interesante manual que denominaré «BreaKcoDe2 «y el grupo de nuevo pone manos a la obra, esta vez se trata de conseguir el crack de Nagra Digital. Lo curioso del caso, en esta historia de Hackers y Crackers, es que al final, se crean verdaderos Cracks a partir de un encuentro con una persona de conocimiento nulo en los sistemas de encriptación, pero que estuvo allí, en un momento apropiado. Pero más curioso aún, es la reacción ultima de este grupo. Todas las aplicaciones obtenidas llevan por sello BraKGroUp, lo que da a entender que el autor es BraKGroUp, es decir, la persona que no tiene conocimientos de Hacking en absoluto.

Se definen a sí mismos como los lideres en nuestro País, y cierran el circulo de amigos a solo unos cuantos programadores que trabajan a merced de BraKGroUp. Lo que se definiría como un bucanero o CopyHacker, ambos descritos en un capítulo anterior.

Esto es así, ya que al cerrarse el circulo, se eliminan los envíos de los ficheros mágicos, sin embargo en la calle estos ficheros «Tarjetas piratas» se venden a precio de oro, es decir, que existen y que alguien los ha sacado a la luz en forma de mercancía. Esto es lo que sé definiría como un grupo de Crackers con intereses económicos y que para nada entra dentro de la ética Hacker. En definitiva BraKGroUp es el caso mas depravante de nuestra historia de Hackers nacionales. En cualquier caso, es el capítulo más oscuro del Hacking Español.

Capítulo 4 Seguridad en Internet, Virus informáticos y otras amenazas

Hablar de seguridad en Internet es como hablar de sí nuestro coche esta seguro en la calle con las llaves puestas en la cerradura. Evidentemente no. Por ello, podemos decir encarecidamente que no existe ningún tipo de seguridad en la gran red de redes. Esto es debido a que quizás, o bien pensaron en una estructura simple «cuando se creo Arpanet» o que quizás hay demasiado listillo suelto por hay.

De cualquier forma, Internet es un lugar donde puedes hacer de todo y paralelamente recibir de todo. Desde descargar un programa de evaluación con éxito a «cogerte» un virus que con un poco de suerte, te dejara fuera de combate por un tiempo.

También es cierto que Internet ha sabido coger muy buena fama para recibir todo tipo de amenazas para tu ordenador, sin embargo en la actualidad se ha constatado la existencia de otras amenazas que no sólo habitan en Internet. En las siguientes paginas conocerá estas amenazas, así como nos centraremos en los virus informáticos, los cuales son mas conocidos por todos nosotros.

4.1. Primero fue el virus, la primera amenaza o fue un Gusano

El primer ataque de Virus del que se tiene información, se registró el 22 de Octubre de 1987 en la Universidad de Delaware en Newark. Según un portavoz del Centro Informático de computadoras de la zona, el virus infecto a decenas de disquetes, por el que se sabe, que el Virus destruyo al menos, una tesis de un estudiante. El virus se llamaba Brain, y cuando se manifestaba, se incluía un mensaje en el cual se pedía a los usuarios que enviaran 2.000 dólares a una dirección de Pakistán para obtener un programa de impunidad.

El virus infectaba el primer sector de un disquete. Los disquetes están segmentados en pequeños sectores y cada uno contiene 512 bytes. El primer sector de un disquete se conoce como «sector de arranque» que es algo así como la parte que permite dar a entender al ordenador que se ha insertado un disquete en la unidad lectora y que en definitiva, contiene datos correctos en su interior. Datos que se

podrán leer posteriormente o áreas del disquete que podrán almacenar nuevos datos, pero lo que realmente nos importa ahora, es la esencia del Boot de arranque del disquete.

El Virus Brain se escondía en este sector precisamente y esperaba a que el ordenador se pusiera en marcha precisamente desde el disquete. De esta forma se creaba un Payload, proceso de carga de un código, en este caso maligno. El payload de Brain consistía sencillamente en poner una etiqueta un tanto especial.

El Virus Brain también contenía un contador que trataba de infectar un nuevo disquete después de que el usuario informático hubiera accedido a él unas treinta veces, todo esto le convertía en un intento de mostrar que se podía hacer algo especial con pocos bytes, pero Brain fue el principio de una plaga más poderosa y malvada.

Poco tiempo después Van Wyk, un asesor informático de la universidad consiguió aislar el «bug» y por decirlo así, encontrar un remedio para paralizar los efectos del Virus de Brain. A dicho remedio, le dio forma de programa ejecutable y le dio el nombre de Antivirus. Pero, fue realmente el Brain el primer virus y Van Wyk el primer creador de un antivirus?.

En 1964, en los laboratorios de Investigación de AT&T Bell, los programadores que allí trabajaban inventaron un juego llamado Core Wars, algo así como una Guerra habida en el núcleo del sistema. La idea consistía en crear un programa que fuera capaz de reproducirse entre sí. Así, dos programadores insertaban dos pequeños programas dentro de un espacio de memoria común, de modo que ambos programas fuesen capaces de reproducirse hasta conquistar la mayor parte de la memoria compartida. Este juego, no fue declarado publico o mencionado hasta 1983, cuando Fred cohen, un legendario programador del MIT, menciono dicho juego y en que consistía. Era esto el primer Iworn de la historia?.

El primer Virus se le escapo a alguien o «lo soltó» deliberadamente en la Red, causando este un colapso en las comunicaciones que entonces se llamaba Arpanet, corría el año 1988 y aquella noche se denomino, la noche que Internet se oscureció.

En realidad se trataba de un iworn o gusano, como quieran llamarle. El creador se sorprendió de los efectos y tuvo que crear otro programa que anulara las funciones de este primero. Así nació, también el primer Antivirus?.

El resultado fue que en solo tres horas el gusano se multiplico dé tal manera que consiguió ralentizar la ReD de Arpanet. Instituciones científicas como la NASA, el laboratorio MIT o el propio ejercito Americano, tuvieron serios problemas en esa fatídica noche. Cinco horas después se descubría que el gusano se difundía a través del correo electrónico, enviando copias de sí mismo hasta oscurecer totalmente la ReD, es decir, colapsarla.

Hasta el momento os hemos contado unas cuantas anécdotas de lo más interesantes, solo han sido tres historias, tres casos que iniciaron una nueva era, la de

los gusanos y los virus. Pero solo se trataba d de la punta del iceberg. En la actualidad surgen cada día unos 100 nuevos «bichos» en la red. De seguir así, para el año 2001 podríamos tener unos diez millones de estos «bichos» en la Red dispuestos a destrozar nuestro disco duro. Esto significa que después de todo, no hay que restarle importancia a las anteriores tres historias contadas. Sin embargo los virus no son la única amenaza que existe, si bien, otras aplicaciones denominadas inocentes, pueden hacernos las cosas un poco más difíciles.

4.2. Pero se especula el origen de los virus mucho antes

La historia anterior descrita se queda enterrada, cuando se conocen nuevos datos sobre quien fue primero y cuando. Sin embargo nos quedamos con el Core Wars, que en esta ocasión parece tener el privilegio de ser el primero puesto en practica después de la idea de John Von Neuman. Mucha gente atribuye la paternidad de los virus informáticos al matemático e investigador en inteligencia artificial, John Von Neuman ya mencionado, quien en 1949 expuso un programa capaz de interaccionar con otros programas diferentes, así como multiplicarse a sí mismo y sobre otro programa, creando así, la destrucción total de un archivo o programa. Dicho de esta manera, se le atribuye el principio de los virus, a la idea del mencionado John Von Neuman, tesis que parece ser puesto en practica varios años mas tarde por Victor Vysottsky, Douglas Mcllory y Robert Morris. Hacia finales de los 60 estos tres hombres crearon un juego llamado Core Wars, siendo este juego mas adelante, el pasatiempo de los empleados del laboratorio de Bell de AT&AT.

El juego consistía en que dos jugadores escribieran sendos programas hostiles, los cuales fueran capaces de crecer en espacio de memoria real. Esta acción se denomina de auto reproducción. Esta idea puesta en practica, permitía que ambas aplicaciones informáticas, se enzarzaran, literalmente en una lucha sin cuartel contra su adversario, buscando un bug en el sistema, para poder replicarse y contagiar al enemigo. Esto implicaba realizar instrucciones invalidas y supuestamente destructoras incluso para el resto del sistema informático. Al termino del juego, la memoria afectada por esta lucha quedaba libre de todo rastro, ya que estas actividades eran severamente castigadas si se detectaban.

Dicho juego permaneció en secreto y uso durante varios años, hacia

aproximadamente el año 1984. En 1983, un año antes de este descubrimiento, alguien llamado Fred Cohen, escribió lo que se conoce como el primer virus después de lo de Core Wars. En 1986 un programador llamado Ralf Burger, descubrió la posibilidad de replicar un ejecutable, pero no fue hasta un año después, que se hizo publico su particular «primer» virus. Todo esto viene a resumir todos los pasos de la creación del primer virus. Un puesto, en el que nadie a ciencia cierta podría asumir. Como todos los descubrimientos de esta vida, todos llegaron primero, pero nadie se atreve a señalar.

4.3. Advert.dll, el espía que esta entre nosotros

Aureate Media es el creador de un pequeño programa, que parece ser, hace de las suyas cuando utilizamos por ejemplo Getrigth o uno de los mas de 300 programas infectados por la idea de Aureate. Este pequeño programa, que al parecer se basa en una librería *.dll, podría estar jugando con los datos de los usuarios.

Así, cuando un internauta se conecta, este pequeño programa podría estar enviando datos de los usuarios a la propia pagina de Aureate o quien sabe donde y para no se sabe que fines. De hecho, la sospecha de este tipo de incidencias sé venia gestando en la comunidad Hacker, desde hace unos cuantos años. Es fácil implicar una segunda función en un programa empleado para Internet como Getright o CuteFTP por ejemplo, sin que el usuario tenga conocimiento.

Para conocer si estamos afectados por este programa, deberemos acceder a la carpeta System de Windows y localizar el fichero Advert.dll, una vez localizado, obviamente tendremos que borrarlo desde MS-Dos. También existe en la ReD, programas especiales como AntiSpy que tras ejecutarlo, realiza la limpieza de este archivo.

Esta practica «la idea de añadir terceras aplicaciones en un mismo programa» parece estar siendo empleada también por el gigante de Microsoft, con su polémico fichero NSA del entorno Windows o el código de identificación del procesador Pentium III, pero estos, son solo algunos ejemplos de como podemos estar siendo espiados y manipulados sin ser conscientes. Lo que os pretendemos decir, es que los virus o los gusanos «iworn» no son las únicas amenazas realmente preocupantes, ya que para combatir a los Virus por ejemplo, disponemos de Antivirus bastante

efectivos que nos protegerán de cualquier amenaza vírica.

Pero que sucede, con estos «Troyanos» de los que estamos haciendo mención en estas líneas. ¿Cómo los detectamos? O como los eliminamos?, «Menos mal que no se trata de Back Orifice 2000 o Netbus». Sin lugar a dudas hay respuestas para todo. Pero es evidente, que también tenemos toda una legión de programas capaces de detectar diferentes caballos de Troya y eliminarlos del PC, incluidos los mencionados entre comillas por ser los más populares. Pero es evidente que no vamos aquí a mencionar todos los Virus, Caballos de Troya o bugs y todos los Antivirus, esto seria añadir paja en todo este asunto y de lo que se trata es de alentaros de los peligros que encierra Internet.

Lo que queda claro es que la mayor amenazas esta en las aplicaciones embebidas a nuestros programas, sino véase los censuradores como WebKeys o los plugins como Third Voice. Son aplicaciones, que aparentemente nos permiten hacer ciertas buenas cosas mientras sé esta conectado a la ReD, pero que emplean complejos Scripts para su funcionamiento, lo que en definitiva se traduce en que estas aplicaciones hacen uso de una base de datos y el intercambio de datos. La polémica esta servida.

4.4. Las amenazas vienen de fuera

La siguiente historia muestra como la amenaza no son los virus informáticos solamente. Existen otros intereses potencialmente peligrosos.

Hace 40 años Nueva Zelanda creo un servicio de inteligencia llamado GCSB «Government Communications Security Bureau» el equivalente a la NSA americana. Ahora y en colaboración con la NSA, crean Echelon. Un avanzado sistema de espionaje a escala mundial, que junto con UKUSA y el empleo de Satélites Intelsat, las nuevas inteligencias gubernamentales pueden desde hace tiempo acceder e interceptar todas las comunicaciones tradicionales como el teléfono, el fax o el correo electrónico.

Esto queda patente desde que en 1996 Nicky Hagar׳s nos muestra otro tipo de espionaje secreto, descubierto en su libro Secret Power, Nicky revela que estamos siendo espiados en todo momento. Según su libro, Nicky afirma que lo que estamos escribiendo ahora es susceptible de ser espiado incluso en el borrador desde nuestro

PC, mediante el método TEMPEST. Este sistema de espionaje aprovecha la radiación electromagnética de la pantalla del monitor para recibir todo lo que se muestra en tal monitor. Por otro lado cuando se termine este articulo y se envíe por el correo electrónico a la sección de Maquetacion, este será inmediatamente interceptado por la estructura Echelon y por supuesto analizado palabra a palabra.

Por otro lado si enviamos un fax a un colaborador o se realiza una llamada telefónica a dicho colaborador para confirmar que se ha recibido el articulo, Echelon también dispondrá de una copia del fax y de la conversación telefónica. Pensar en todo esto, simplemente le pone a uno los pelos de punta.

En 1948 se formaliza UKUSA después de interceptar varias comunicaciones de radio secretas durante la segunda guerra mundial. Junto con Echelon, UKUSA «denominada Spy Network» potencia las posibilidades de controlar las comunicaciones globales desde los satélites Intelsat.

El jueves, 12 de junio de 1984, Rob Muldoon conviene en el parlamento lo que seria el primer paso para crear Echelon. Diez años mas tarde, el 15 de enero de 1994 los técnicos de satélites interceptan comunicaciones extrañas en los satélites, fecha en la que se revela la existencia de UKUSA.

Desde entonces todas las comunicaciones son interceptadas por Echelon y Ukusa y descifradas por técnicos expertos en busca de información confidencial de un posible movimiento militar, terrorista o de otra índole.

Todo esto bien podría parecer una película de Ciencia-Ficción pero lo cierto es que no es así. Europa ya dispone de Enfopol, la respuesta a Echelon y Rusia anuncia su propio sistema de espionaje a gran escala. Parece que la guerra fría deja paso a la guerra tecnológica en un tiempo en el que predomina el poder de la información y la obsesiva idea de que nuestro vecino esta urdando un plan de invasión inminente.

Sin embargo Echelon, Enfopol u otras organizaciones tecnológicas no son las únicas amenazas a tener en cuenta o que existen, sin ir mas lejos, Bill Clinton se empeño hasta hace bien poco en incluir el Clipper chip en los aparatos de teléfono, a fin de poderintervenir la comunicación deseada. El Clipper chip es un codificador seguro contra Hackers, pero que dispone de una puerta de atrás para todos los efectos de los gobiernos, es decir, la CIA o simplemente la policía federal, puede descifrar la comunicación con una segunda clave.

Finalmente el Clipper Chip no parece haberse incluido en los aparatos de teléfono, aunque las dudas quedan de sí están implantados en los teléfonos celulares. Lo que sí es cierto, es que Windows viene acompañado de un archivo denominado NSA que según el propio Bill Gates, se trata de una clave coincidente con la realidad de ser una puerta trasera por la que la NSA puede entrar en tu ordenador. Bueno, la duda sigue en pie aun a día de hoy.

Estas declaraciones sirven para mostrar todos los tipos de amenazas que

conocemos, ademas de los devastadores virus informáticos. Particularmente me afectan tanto los virus mencionados como los Backdoor o puertas traseras, que el estado y los fabricantes, incluyen en nuestros sistemas informáticos.

4.5. El verdadero rostro de Internet

Lo que leerá en los siguientes párrafos es una amenaza que viene desde fuera, y que por su efecto negativo, lo incluiré como amenaza para todos los usuarios del teléfono, el Fax e Internet. En definitiva, todo lo expuesto en estas paginas es un gran acercamiento a la realidad de Internet, el nido de las pesadillas del internauta. Todo comenzó en 1962, que, anticipándose a las consecuencias de un desastre atómico, el ejercito del Aire de los Estados unidos le encargo a un reducido grupo de ingenieros, crear una ReD de comunicación que aguantase un ataque nuclear. Obviamente los ingenieros mostraron rostros pálidos, pero la idea gusto y fue así como nacía Arpanet.

Eso sí, no precisamente ese año, ya que Arpanet veía la luz en 1969. La culpa de este retraso, la tuvo la falta de visión del Pentágono. Después de dos intentos de lanzar la ReD, el Pentágono cedió, quizás sin saber que años mas tarde, sus defensas electrónicas cederían ante los miles de ataques de Hackers de todo el mundo.

La ReD esta formada de miles, millones de nodos, de modo que si bombardean un país y con él, miles de nodos, siempre existirán otros nodos para seguir manteniendo una comunicación abierta. Sin embargo, el pequeño grupo de ingenieros no tuvo en cuenta la Guerra electrónica y los propios Hackers. Un simple Gusano «iworn» puede colapsar la ReD en pocas horas. O en el mejor de los casos, un simple virus puede ser enviado a millones de maquinas conectadas en todo el mundo.

Para finalizar este bloque solo queda aclarar que la idea a manifestar en esta nueva entrega de la comunidad Underground-Tecnológica, es que Internet esta plagada de pesadillas para nuestros ordenadores, que no son necesariamente los virus lo que hay que temer, que tampoco nos pueden asustar los Caballos de Troya, sino las «aplicaciones» oscuras que algunos programas comerciales contienen y en definitiva, el ojo avizor que nos espía desde el cielo.

4.6. ¿Quiénes son ellos?

Ellos en un principio son muchos y muy variados. Son los nuevos personajes de una nueva sociedad underground o ciberdelincuentes en la mayoría de los casos. Pero es evidente que no podemos echarle la culpa a todos, de lo que pasa en la red.

En Internet existen, principalmente internautas que se pasan largas horas delante del ordenador buscando atractivas imágenes de mujeres desnudas, otros simplemente buscan algún tiempo de información para terminar un trabajo, otros buscan la sinopsis de la ultima película de Spielberg, pero una pequeña minoría se pasa largas horas entrando en sistemas con el fin de lograr sus objetivos basados en satisfacciones personales. Entrar en un lugar supuestamente «seguro», los que lo consiguen simplemente se sazonan de alegría, una diminuta minoría se queda en el lugar y fastidia todo lo que ve a su paso.

Dentro de esta galería de personajes podemos nombrar a los sencillos internautas, los Hackers, Crackers o los Lamers entre una devastadora familia de intelectuales expertos en temas informáticos. Pero de todos ellos ya hemos hablado, ahora lo que realmente importa, es saber quien programa virus. Esta es la pregunta del millón, algunos se dan a conocer y otros, sencillamente son detenidos, después de que su virus cause un caos general en el mundo de Internet. Ademas, es importante conocer como son y como actúan los virus informáticos, así como conocer la forma de protegerse de ellos. En este capitulo, ademas de incluir algunas batallitas o historias sobre creadores de virus, tendremos la simpatía de explicarle que son y como funcionan los virus informáticos.

En realidad, es parte importante conocer estos últimos terminos, ya que ademas le daráuna clara idea de lo que se puede encontrar en Internet «véase Virus informáticos y otras amenazas», y sobre todo, tendrá la certeza de como actuar frente a un contagio.

4.7 Pesadilla en la ReD

Podemos enumerar una gran lista de amenazas que pondrían los pelos de punta a mas de uno, pero no se trata de eso. Mi obligación como escritor es informar y dar detalles de las diferentes amenazas que han surgido en la Red en los últimos años, no

sin ello desalentar al futuro o actual internauta a engancharse a la red.

Todo lo que quiero explicar es, para que el internauta adquiera la conciencia de la existencia de ciertos peligros y los suficientes conocimientos, como para estar preparado frente a lo que se puede encontrar y donde encontrarlos. Es algo así, como formar un experto a distancia, para prever que le fastidien su ordenador o recibir una sorpresa, que lo único que aporta es un buen cabreo.

En Internet es posible navegar a través de paginas WEB denominadas World wide Web. Otra opción es la del correo electrónico, el cual nos facilita la comunicación entres las personas a través de texto, pero las ultimas tendencias permiten enviar vídeo además de texto, así como audio, por lo que las comunicaciones a través de Internet nos ofrecen claras ventajas a los tradicionales métodos de comunicación como el teléfono, por ejemplo.

Otro de los objetivos de Internet «el principal» es que cualquier ordenador también pueda conectarse o comunicarse con otro cualquiera desde cualquier punto del planeta.

Por ello en un principio, ese era el principio de la idea imponible y como los ordenadores conectados en red «en aquel momento» eran principalmente los de las principales instituciones de estudios e investigación, se tomo pocas precauciones de seguridad, salvo los password de acceso.

El problema vino después, cuando la red de Arpanet se convirtió en una red más grande llamada Internet, que permitía el acceso a cualquier internauta para consultar unas simples paginas de una sede. Después llegaron otras opciones, como correo electrónico, y servicios FTP entre otras. Pero estos servicios no fueron la causa del nacimiento de los primeros Hackers o sociedad ciberpunk.

El problema vino después, cuando a alguien se le «escapo» literalmente un programa a través de la red, que poseía la opción de autoreplicado de sí mismo. El cual causó unembotellamiento de las comunicaciones de esta red, ya que el programa sé autoreplicaba con tal velocidad que colapsaba las comunicaciones como si miles de nuevos internautas se sumaran a la red al mismo tiempo.

Para eliminar el problema, hubo de crearse otro programa que contrarrestara las funciones de dicho programa autoreplicante. A este incidente se le denomino «gusano» y a la solución al problema «vacuna».

Así nació el primer virus y el primer antivirus.

4.8. Los virus informáticos

Los virus son la principal amenaza en la Red. Estos programas de extensión relativamente pequeña, son programas capaces de autoreplicarse o dicho de otra manera, son capaces de hacer copias de si mismo en otro archivo al que ocupa. Este método bloquea y llena el disco duro de un PC.

Otros virus además poseen funciones de modificaciones en los principales ficheros del sistema operativo de nuestro ordenador. Pero los hay también benignos que solo muestran mensajes en la pantalla. Nos detendremos a estudiar los diferentes tipos de virus y analizaremos algunos de ellos, como los a tener en cuenta.

Los virus poseen unas particularidades que los hacen perfectamente reconocibles por la forma en que trabajan, los virus poseen un proceso de creación, incubación y reproducción.

4.9. La vida de un virus

El virus se crea o nace, esta claro en el ordenador del creador como subprograma o microprograma ejecutable. Después este se «suelta» en la red o se copia «inserta» dentro de un programa comercial de gran difusión, para asegurar un contagio rápido y masivo.

Después de esta primera fase de creación, vienen las más importantes a cumplir de forma automática e independiente del control de creador del virus, «principalmente creado por un enfadado empleado recientemente despedido de la empresa en la quetrabajaba y que guardaba esta carta bajo la manga» este proceso consta de contagio, incubación, replicación y ataque.

4.10. El contagio

El contagio es quizás la fase mas fácil de todo este arduo proceso. Solo hay que tener en cuenta que el virus debe introducirse o «soltarse» en la red. El virus debe ir incrustado en un archivo de instalación o en una simple pagina WEB a través de los cookies.

Las vías de infección son también principalmente los disquetes, programas copiados, Internet o el propio correo electrónico, en este ultimo caso el contagio es considerado como masivo y por lo tanto, muy peligroso, véase virus Melissa o I Love You.

4.11. La incubación

Normalmente los virus se crean de formas especificas que atienden a una serie de instrucciones programadas como el «esconderse» y «reproducirse» mientras se cumplen unas determinadas opciones predeterminadas por el creador del virus.

Así, el virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan las condiciones determinadas por el creador. Este proceso puede ser muy rápido en algunos casos y bastante largo en otros, según el tipo de virus.

4.12. La replicación

La replicación consiste en la producción del propio virus de una copia de si mismo, que se situara en otro archivo distinto al que ocupa. De esta forma el virus se contagia en otros archivos y otros programas, asegurándose de que el proceso de multiplicación esta asegurado.

Además, el virus asegura su extensión a otros ordenadores y debe hacerlo de la forma más discreta y rápida posible. En este momento el virus no se manifiesta, ya que solo se instala en cuantos más lugares mejor.

Solo de esta forma, mas posibilidades tendrá de dañar un mayor numero de ordenadores.

4.13. El ataque

Cuando se cumplen las condiciones, efectuadas por el creador del virus, este entra en actividad destructora. Aquí es donde formatea el disco duro o borra archivos con extensión COM o EXE por citar algunos ejemplos.

El ataque es el escalón final del trabajo del virus. Cuando se llega a este punto el trabajo ha culminado. El ordenador se encuentra infectado y si no se dispone de un programa que elimine el virus, jamás se podrá recuperar los archivos. Podemos instalar de nuevo el software, pero de nuevo tendremos la destrucción de nuestra unidad nada mas se cumplan los acontecimientos antes citados.

Estos programas capaces de destruir el virus, se denominan vacunas antivirus.

4.14. Pero, son todos lo virus iguales

Indudablemente no.

Estamos ante unos programas bastantes inteligentes y obviamente creados por diversas personas con ideas y fines distintos. Los virus, son denominados así, para conocimiento común, pero no todos ellos reciben este nombre. Entre la extensa familia de virus que existen con diferentes manifestaciones, hay que destacar otra extensa galería de subprogramas inteligentes que pueden actuar como virus con fines diferentes al de fastidiar únicamente el disco duro del ordenador.

Por ejemplo tenemos programas que únicamente se encargan de robar los password de nuestro ordenador, otros simplemente llenan el disco duro y otros tantos se dedican a mostrarnos multitud de publicidad en nuestro correo electrónico hasta

saturarlo. Todos ellos serán mencionados en este libro y trataremos de explicar que son y que hacen cada uno de ellos.

Entonces entra la sugestiva pregunta de si todo lo que se sale de lo normal en la red son virus, como respuesta diremos que no, ya que además de estos virus, podemos citar los Caballos de Troya, las bombas lógicas o los Spam por ejemplo.

4.15. Los caballos de Troya

Son programas que normalmente ocupan poco espacio y se «cuelan» a voluntad en el interior de un ejecutable. Este subprograma se coloca en un lugar seguro de la maquina para no ser detectado y no modifica nada de los archivos comunes del ordenador y cuando se cumplen unas especificaciones determinadas el subprograma muestra unos mensajes que sugieren o piden la contraseña al usuario de la maquina.

En otros casos simplemente lee el password cuando nos conectamos a la red, tras copiar el password, este sé encripta y se envía por correo electrónico adjunto. El Hacker lo que debe de hacer ahora es «capturar» ese mensaje y descifrar su propio código.

El mensaje es fácilmente capturado, mediante un sniffer, esto es, un programa de monitorizado de la red, pero los mas expertos emplean caballos de Troya más inteligentes, que lo que hacen es reenviar o «desviar» el mensaje a una dirección del Hacker sin que el usuario sé de cuenta.

4.16. Las bombas logicas

Son una de las buenas bazas del Cracker «malicioso» al igual que un virus las bombas lógicas están especialmente diseñadas para hacer daño. Existen dos definiciones del mismo acrónimo o programa asociado. Una es la de crear un

subprograma que se active después de un tiempo llenando la memoria del ordenador y otra es la de colapsar nuestro correo electrónico.

De cualquier forma ambos son dañinos, pero actúan de forma diferente. En la primera referencia, este se instala en nuestro ordenador después de ser bajado junto a un mensaje de E-Mail. Se incuba sin crear ninguna copia de sí mismo a la espera de reunir las condiciones oportunas, tras ese periodo de espera el programa se activa y sé autoreplica como un virus hasta dañar nuestro sistema. En el caso segundo, alguien nos envía una bomba lógica por E-Mail que no es sino que un mismo mensaje enviado miles de veces hasta colapsar nuestra maquina. Los programas antivirus no están preparados para detectar estos tipos de bombas lógicas, pero existen programas que pueden filtrar la información repetida. De modo que la única opción de fastidiar es hacer «colar» una bomba lógica que se active frente a determinadas circunstancias externas.

4.17. Los gusanos «Worm»

Son programas que tienen como única misión la de colapsar cualquier sistema, ya que son programas que se copian en archivos distintos en cadena hasta crear miles de replicas de si mismo. Así un «gusano» de 866 Kbyts, puede convertirse en una cadena de ficheros de miles de Megas, que a su vez puede destruir información, ya que sustituye estados lógicos por otros no idénticos.

Los gusanos o «Worms» suelen habitar en la red a veces como respuesta de grupos de «Hackers» que pretenden obtener algo. La existencia de uno de estos gusanos se hace notar, cuando la red se ralentiza considerablemente, ya que normalmente el proceso de autoreplicado llena normalmente el ancho de banda de trabajo de un servidor en particular.

4.18. Los Spam

No se trata de un código dañino, pero si bastante molestoso. Se trata de un simple programa que ejecuta una orden repetidas veces. Normalmente en correo electrónico. Así un mensaje puede ser enviado varias cientos de veces a una misma dirección. En cualquier caso existen programas, antispam, ya que los spam son empleados normalmente por empresas de publicidad directa.

4.19. Volviendo a los virus informáticos

Internet aporta, lo que se podría decir una vía rápida de infección de este tipo de programas dañinos. Antes, la distribución o infección de los virus, era algo mas que una tarea lenta y ardua, ya que solo se contagiaban a través de disquetes. Por ello, la Red bien podría llamarse el gran nido.

Después de explicar las distintas fases, desde la creación de un virus, tenemos que enumerar al menos que distintos tipos de Virus coexisten actualmente en la Red. No sin antes dejar comentado, que tal como están puestas las cosas hoy por hoy, surgen cadadía unos 100 nuevos «bichos» en la red. De seguir así, para el año 2.000 podríamos tener unos diez millones de estos «bichos» en la Red dispuestos a destrozar nuestro disco duro.

A esto hay que añadir la metamorfosis de los nuevos virus cada vez más inteligentes y a las tres vías de propagación mas ampliamente conocidas, como son por un attach de correo electrónico, un trasvase FTP o un download desde una pagina WEB. Con todas estas circunstancias, podríamos atrevernos a decir que la red estará gobernada por millones de formas capaces de bloquear cualquier sistema, dado además, por los varios tipos de virus que existen.

4.20. Tipos de Virus

Existen al menos cinco tipos de Virus conocidos hasta ahora, esto no quiere decir que están todos, seguramente mientras escribo estas líneas habrá surgido algún que otro engendro mas sofisticado. Pero básicamente son estos:

* Virus de arranque o Virus de Boot.
* Virus de Macro.
* Virus de ficheros.
* Virus polimórficos.
* Virus multiparte.

A la presente lista podemos añadir los Virus Hoaxes que no son realmente lo que representan ser, hablaremos mas adelante de ellos.

Los Virus de boot o de arranque eran hasta los 90 los típicos virus que infectaban el sector de arranque del disco y estos eran introducidos al ordenador a través de disquetes.

El modo de funcionamiento es básico, al arrancar la computadora, el virus se instalaba en la memoria RAM antes que los ficheros del sistema INI, de esta forma podían «fastidiar» a su antojo lo que querían.

Para no ser detectados, estos virus de Boot, se copiaban a si mismos en otro lugar del disco duro, con el fin de no ser descubiertos.

Los virus de Macro están mas elaborados y son virus escritos a partir del macrolenguaje de una aplicación determinada. Por ejemplo podemos citar el Word, procesador de textos. Estos virus, son realmente dañinos, porque son capaces de borrar un texto, dado que los bloques macro son diminutos programas del propio Word, por ejemplo, que permite ejecutar varias funciones seguidas o a la vez con solo activar la casilla.

Por ello un Macro programado con la instrucción deshacer o borrar, resultara «hermosamente» dañino. Otros sin embargo, podrán resultar inofensivos, dado que son programados con funciones de copiar y pegar por ejemplo, no perdemos datos, pero si resulta algo bastante molesto.

En el caso de Acces, esto se complica, ya que este programa permite además de códigos Macro, programar Scripts. Los scripts son invocados según unas determinadas funciones, por ejemplo la tecla A pulsada tres veces ocasiona la ejecución de un Macro. Por otro lado, eliminar los virus o scripts malintencionados puede resultar una tarea bastante compleja, ya que reemplazar o desactivar no solo los comandos Macros si no también los scripts, puede causar que algunas funciones básicas del programa dejen de funcionar.

Los Virus de Fichero son conocidos también como «parásitos» y suelen operar desde la memoria tras haber tomado control de los ficheros o archivos ejecutables, como las extensiones COM,EXE, DLL o SYS.

Se activan solo cuando se ejecuta algunos de estos ficheros, permanecen ocultos y estallan después de unas determinadas funciones programadas.

Los virus polimórficos son aquellos que son capaces de cambiar de estado o la propia cadena de datos. De esta forma el mismo Virus puede verse dividido en varias secciones repartidas en varios ficheros, pero a causas naturales actúa como tal. Estos Virus son difícilmente localizables y solo en excepciones, los método heurísticos podrían detectarlos en el caso de que algún fichero crezca demasiado de tamaño.

Estos virus pueden estar encriptados y muy bien repartidos por decenas de ficheros, con lo cual se convierten en los virus más peligrosos, dado que pueden ser programas largos. Los virus multiparte, están conformados a base de Virus tipo boot que operan desde la memoria y virus de Fichero, que infectan extensiones ejecutables. Estos Virus también pueden burlar los modernos métodos heurísticos de búsqueda de los programas de antivirus.

4.21. Otras amenazas

Dejando a un lado los temibles Virus y los caballos de Troya, existen otras amenazas en la red prediseñados para monitorizar el trasvase de datos en la línea y de hay tomar prestados algunos paswords o números de tarjeta de crédito.

Estos programas capaces de monitorizar a alguien en particular o todo aquello que se mueve en la red, recibe el nombre de sniffer y como su nombre indica, son programas capaces de interpretar todos los datos de la red, copiarlos y modificarlos.

Otras amenazas son los buscadores de puertos libres IRQ, con estos programas se pueden localizar puertos libres o abiertos y entrar por ellos a otros sistemas. A veces estos puertos contienen Bugs, «fallos» y los Hackers las emplean para penetrar en los sistemas.

4.22. Cómo se que estoy contagiado por un Virus?

Una de las preguntas más frecuentes de cualquier internauta o usuario de ordenadores es, ¿Cómo detecta un posible contagio de un Virus?. Evidentemente si esta contagiado de un Virus fatal y este se activa nada mas contagiarse, sé verán los efectos devastadores de una forma radical. Normalmente los virus maliciosos te muestran una ventana de bienvenida y en la que se te informa del contagio, después el virus hace su faena de destrucción. Pero, ¿Que pasa si esta infectado por un Virus que actúa mas adelante?. En este caso, los síntomas son bien diferentes. En la siguiente lista puede ver algunos de los síntomas más importantes.

1. Se pueden sufrir caídas frecuentes del sistema sin causa aparente, estas caídas están basadas en mensajes de error o aplicaciones que no responden, así como fallos al arrancar una aplicación.

2. Puede observar una reducción considerable del espacio de su disco duro, así como de la memoria RAM. Esto ultimo es debido a que cuando un virus es activo, este ocupa parte de la memoria RAM para poder ejecutarse. Si parte de esta memoria esta ya ocupada, tenemos como resultado una inestabilidad de nuestro sistema, con síntomas que implican mensajes de falta de memoria.

3. Puede observar la desaparición de archivos o cambio en el tamaño de los mismos, así como la extensión que puede verse afectada.

4. Es posible que un fichero EXE cambie de tamaño, ya que el virus se ha replicado en él. Después este ejecutable puede presentar anomalías de tiempo tras arrancar, lo que implica la ejecución del virus.

5. Puede observar cambios y situaciones extrañas en su pantalla, ya que algunos Virus están programados para actuar en el sistema de vídeo. Esto implica que si observa cualquier desajuste de la pantalla es porque esta infectado. Otros virus más agresivos, se manifiestan invirtiendo el video, como si este se reflejara en un espejo o se situara del revés. Algunos de estos virus o efectos, pueden ser obra de una broma, que se extingue cuando se pulsa una tecla cualquiera.

6. Es posible que cuando pulse determinadas teclas. Vea acciones extrañas en su PC, esto es debido a que algunos Virus se basan en la pulsación de dichas teclas para activarse.

4.23. Desinfectando, los Antivirus

En la actualidad podemos decir que estamos de enhorabuena, ya que se disponen de muchas y variadas formas de defenderse de los virus informáticos, es decir, que existe gran variedad de software Antivirus. Los Antivirus son programas específicos, capaces de detectar y eliminar la mayoría de los virus. Digo mayoría, ya que un Antivirus debe de ser constantemente actualizado, ya que cada día aparecen nuevos y más enigmáticos virus informáticos. En este sentido, se hace difícil elegir el Antivirus adecuado, pero encualquier caso, cualquier elección será siempre mejor que no tener instalado uno de ellos en nuestra computadora.

Para desinfectar nuestra computadora de cualquier virus, tenemos que tener cierta noción de como funcionan y actúan los Antivirus. En la siguiente lista podrá observar diferentes situaciones, las cuales le permiten detectar cualquier tipo de virus, sea cual sea su naturaleza.

1. Si detecta, por los síntomas, que el virus se ha instalado en la memoria RAM, deberá reiniciar su computadora, con el fin de que el Antivirus chequee el boot de arranque del sistema, así como la RAM. También es cierto que por ejemplo, el Antivirus de Panda, permite chequear esta zona sin necesidad de reiniciar su PC.

2. Si ejecuta el Antivirus, por lo general, le permitirá chequear todos los discos duros de su maquina, disqueteras, así como unidades lectoras de CD o correo electrónico. Todo esto lo podrá chequear desde la opción Setup del Antivirus. Si en este chequeo detecta algún tipo de Virus el Antivirus procederá a desinfectar el fichero infectado, sin necesidad de alterar el funcionamiento de dicho fichero infectado.

3. Algunos Antivirus, permanecen activos todo el tiempo, por lo que sí resulta infectado por uno de ellos, el Antivirus lanzara un mensaje de alarma indicándole que tipo de virus ha sido detectado. Cuando aparezca este mensaje opte por desinfectar su aplicación.

Como ha podido comprobar el uso de Antivirus no es nada complejo, ademas dichas aplicaciones están tan automatizadas, que tras la instalación, el usuario puede olvidarse de los virus. Lo que sí debe tener en cuenta, es que debe actualizar su antivirus de forma constante, algo que se hace mediante una conexión segura a Internet.

4.24. Una rápida Guía de Virus mas conocidos

Para terminar que mejor que exponer una pequeña guía de los virus más devastadores de la historia, y por lo tanto, mas conocidos. Esto le evitara caer en la trampa de ejecutar algunos archivos que le llegan a través del correo electrónico. Recuerde que la mayoría de las infecciones de virus en la actualidad, llega por la vía del correo electrónico y tras ejecutar el fichero adjunto al mensaje. En los últimos días también se conoce una versión de virus que se aloja en una película de Flash de Macromedia, por lo que es posible ser infectado con solo visitar una pagina Web que contiene Flash. Con esto no quiero decir, que Flash es la única vía de contagio cuando se habla de paginas Web afectadas. También los Java Scripts o Applets de Java por portadores de peligrosos virus. Por orden cronológico, en la siguiente lista conocerá algunos de los virus más conocidos y potencialmente conocidos

1. 1986 . En este año se conoce el virus Virdem, no es el primero, pero si el primero que infecto a una serie de ordenadores que sufrieron su efecto poco después.

2. 1986. En este mismo año se conoce a Brain, un virus que copiaba esta palabra tras arrancar el ordenador.

3. 1988. Es el año que se lanza el virus mas conocido de la historia, se trata Viernes 13. Este virus se manifiesta todos los Viernes 13 y propicio la aparición de los primeros Antivirus.

4. 1995. No es ni mucho menos el siguiente virus al viernes 13, pero si el año en que aparece Ping Pong. Se recuerda a este virus por su particular forma de mostrarse. Se trataba de hacer aparecer una bola de Ping Pong rebotando en toda la pantalla. El virus no era realmente dañino, pero sí bastante fastidioso.

5. 1995. En este mismo año aparece barrotes, un virus potencialmente peligroso por sus efectos, ya que como su nombre indica, se mostraba en forma de barrotes. Esto daba lugar a que buena parte de la información se veía infectada.

6. 1995. En este año aparece también el virus Holocausto también denominado Virus potencialmente peligroso por sus efectos.

7. 1999. Es el año más prolífico en cuanto a virus potencialmente dañinos, a las puertas del caos del efecto 2000 informático, aparece el virus Melissa. Este es un virus de Macro, que tras infectarse por medio del correo electrónico, se propaga a las primeras 50 direcciones de correo electrónico y así sucesivamente. La velocidad con que se multiplica este virus, permite un colapso total en decenas de miles de ordenadores.

8. 1999. 1999 parece ser el año del caos y de las predicciones. En este mismo años aparece el que se conoce como el virus más malicioso jamás creado. Se trata del chernobil, un virus capaz de afectar al hardware de nuestra maquina, reescribiendo incluso en la Flash de la Bio del sistema. 9. 1999. Plagado de fatalidades el año continúa con I Love you. Junto al gusano VBS.BUBBLEBOY, este virus es el que más ordenadores a afectado. Su rápida propagación por el correo electrónico permitió

a este virus, colapsar una vez mas la red de Internet.

10. 2000. Es el año donde apogean las tarjetas piratas de televisión de pago. Año en que se crean círculos cerrados de investigadores de estos sistemas digitales. El enanito se envía a través de estos círculos de forma continuada, si el usuario lo confunde por un file de claves, este queda potencialmente dañado con un formateo del disco duro. La intención de este virus es eliminar todos los archivos relativos a crear tarjetas piratas para ver televisión de pago de una forma fraudulenta.

Capítulo 5 Una pequeña, pero amplia recopilación de extractos de reportajes sobre Hackers.

Un título un tanto extraño se dirá, a sí mismo. En realidad lo que se pretende decir en tal largo titulo, es que en el presente capítulo encontrará párrafos extraídos de algunos de mis reportajes sobre Hackers, que fueron publicados en su día y que ahora recupero, para este libro, dado que los considero muy importantes por su contenido. Dichos extractos podrían ser muy bien, una recopilación de «hazañas» sobre Hackers. En parte así es, y en parte también trato de describir un poco mas, que es un Hacker y lo que es la noticia acerca del Hacker.

Sin seguir un orden cronológico, en las siguientes líneas incluiré párrafos explícitos, historias de Hackers, hechos y lo mejor de mis reportajes en este tema. Para los que siempre se interesaron por seguir mi obra, reconocerán gran parte del material aquí expuesto, mientras que creo, que también existirá un pequeño grupo de personas, que encontraran aquí, aquellos escritos que tanto ansiaban leer. En definitiva, espero que disfrute con el contenido de este capitulo, que más que dar quebraderos de cabeza, para comprender un algoritmo de cifrado o entender el funcionamiento de un Virus, os mantendrá en vivo ese espíritu de interés, durante unos momentos, que espero sean muy gratificantes.

5.1. Recopilación primera Crackers «rompedores» de la televisión

AD B1 34 33 D3 F5 58 59 «Key primaria» …Este es el lenguaje que emplean los nuevos Crackers en los Foros dedicados a Seca y otros sistemas de encriptación digitales. Estos nuevos «rompedores» de las leyes de la criptografía y de los algoritmos son los dueños de la nueva televisión de pago. En este reportaje conocerá la capacidad de estos «genios» para hacerse con la tecnología de encriptacion.

Son las 19:30 de la tarde y uno a uno, se van cerrando los diferentes canales de una conocida plataforma Digital. Es el momento de los cambios de las Keys. En el Descodificador esta insertado la tarjeta Gold Card ejecutando su habitual rutina de desencriptado, pero ya no se puede ver nada en la pantalla del televisor, excepto una negrura total… parece como si de repente hasta el televisor ha dejado de funcionar.

Pero no hay que alarmarse, pues todo este proceso es normal excepto para los que poseen una tarjeta Autoupdating ya que hay que reprogramar de nuevo la tarjeta, es decir, hay que aplicar las nuevas Keys. Esto no es un problema ya que las nuevas Keys están disponibles desde hace un mes y además han sido testeadas hace unas cuantas horas.

Todo esto esta en Internet, en paginas difíciles de memorizar, pero no imposibles, que están ubicadas en servidores donde las nuevas leyes Europeas no surten efecto alguno, es decir Rusia. Ahora el usuario de este tipo de tarjetas deberá introducir los nuevos ficheros en la Eeprom de su tarjeta con la ayuda de un programador económico. Los mas avispados actualizan sus tarjetas desde el mando a distancia de su descodificador, si, desde el mando a distancia, tan sencillo como eso, y cinco minutos mas tarde ya pueden ver de nuevo todos los canales de televisión.

Las nuevas Keys ya han sido introducidas en la tarjeta pirata y todo vuelve a la normalidad. En el otro extremo de Internet, los Crackers comienzan la gran tarea de buscar las nuevas Keys para el próximo mes. Pero se acaba de anunciar la SuperEncriptacion, significa esto que los Crackers tienen los días contados, según ellos la SuperEncriptacion es solo un paso mas, el espectáculo esta servido.

5.2. Recopilación segunda Cracks, lo que realmente motiva

Crack, sinónimo de ruptura, siempre se ha asociado a las catástrofes o la caída de sistemas, ya sean económicos o físicos. Una economía hace Crack, cuando esta cae por los suelos. Un ser humano hace Crack cuando este fallece. Crack también se utiliza para identificar la caída de un sistema informático. En definitiva, el termino Crack es utilizado siempre que algo termina, se rompe o deja de funcionar. Para los Crackers, Crack es el comienzo de una nueva era.

Inusual entradilla esta la de arriba, pero contundente en las descripciones. Sin llegar a acordarse uno de fechas fatídicas o eventos históricos, lo cierto es que la palabra Crack a sido asociada a estas desgracias mas de una vez, en la historia del hombre. Ahora, sin embargo, con la llegada de la informática y el asentamiento de esta, el termino Crack, cobra nuevo sentido o quizás es mas conocido por todos los mortales.

Directamente ligado a los Crackers, el Crack es la revelación de sus conocimientos y habilidades. Directamente podríamos decir sin temor a equivocarnos, que el Crack, es el éxtasis del Cracker, su punto de culminación. Para los fabricantes de Software y de electrónica, el Crack, es su peor amenaza, la peor de sus pesadillas.

Mientras se urden las grandes telarañas de la leyes de aquí y allá, los Crackers se revelan contra la tecnología, ofreciendo sus conocimientos en la red. Estas acciones responden a la ideología de la libertad de información y los Crackers las defienden con uñas y dientes.

Otros, simplemente Crackean sistemas por diversión. Otros tantos, hacen Cracking al servicio del Don dinero o a las ordenes del gobierno. Estas son pues, las diferentes caras del Cracking, la terminología Crack y los propios Crackers.

5.2.1. Un punto de reflexión sobre los Cracks

Antes de continuar debemos de conocer perfectamente lo que es un Crack y cuando surgió esta idea. Un Crack es la rotura total de un sistema, ya sea de Software o Hardware. Los que realizan tales Cracks, son denominados Crackers, y son un eslabón mas de los Hackers. Si los Hackers son capaces de penetrar en los sistemas informáticos, los Crackers son capaces de desproteger el mismo sistema informático.

El inicio de los Cracks no se gesta con el Software como se cree. Mucho antes de que conociéramos Windows, aplicaciones de fotografía, editores HTML y un gran numero de aplicaciones de Software que hoy día conocemos, los Cracks ya se habían hecho un hueco en el mundo Underground. Pero entonces se denominaban Phreakers «rompedores de sistemas telefónicos» y ahora simplemente Crackers o HardwareCrackers. La acepción acertada quizás no exista todavía, pero si se pueden distinguir los diferentes grupos de Crackers que existen en la actualidad y que parecen estar divididos en varios grupos.

5.2.2. Los Cracks de Software

Programas tan importantes como 3D Studio Max, Photoshop 5.5, Dreamweaver 3 o Windows Millenium, corren por Internet completamente desprotegidos, es decir, no se caducan o están registrados de forma fraudulenta. Son los denominados Warez o Appz. Ambas terminologías están siendo utilizadas para definir un Software desprotegido y libre de pagos. Simplemente debes de tener un poco de paciencia al descargarlos de Internet, ya que se encuentran completos y por lo tanto estamos hablando de varios Megas interminables de descarga.

En otras zonas de Internet, encontraras, sin embargo, pequeños Pacth´s que te permitirán desproteger el mismo Software, si te encuentras «rulando» una Demo. Estos «parcheadores» son simples programas ejecutables, cuya única tarea consiste en sustituir unas cuantas líneas de código dentro del ejecutable.

Estos últimos son los denominados Cracks de Software y son los que mejor tienen planteada su supervivencia en la red, ya que son programas pequeños, que pueden ser descargados de forma rápida y además cuentan con un funcionamiento muy sencillo. Tan sencillo como iniciar el programa dentro de la carpeta donde se encuentra la Demo y aceptar.

Para los Crackers, esta es una forma de hacer llegar la tecnología a todo el que la desee probar, al tiempo que se convierte en un reto el desproteger un Software cada día mas protegido.

5.2.3. Un HardwareCracker

El HardwareCracker nace antes que el propio Cracker, es decir, aquel que desprotege sistemas informáticos como Software. El HardwareCracker comienzo su andadura «desprotegiendo» sistemas telefónicos y se gano el acrónimo de Phreaker, pero a día de hoy, las nuevas tecnologías aportan un nuevo reto para estos genios de la electrónica. La televisión digital, los sistemas de anticopiado de vídeo o las tarjetas inteligentes, son los nuevos pasteles para el Cracker. En este caso, el Cracker debe tener unos conocimientos muy elevados de electrónica ya que debe modificar circuitos electrónicos, es decir, Hardware. Por ello el acrónimo de HardwareCracker.

En la actualidad el HardwareCracker también está presente en Internet. Si buscas

información sobre sistemas de televisión de pago, es fácil encontrar en la red paginas llenas de circuitos electrónicos que te permiten desproteger esos «canales de pago». En este caso, aunque también puedes bajarte dicha información a tu ordenador, el realizar el Crack implica tener un poco de conocimientos de electrónica por parte del internauta para poner en marcha el mencionado Crack. Pero aun así, la nueva sociedad parece estar preparada para ponerlos en practica con pocas dificultades.

5.2.4. Crackers al servicio del gobierno

El Crack realizado para los intereses de un gobierno y de un país entero, fue el descubrimiento del funcionamiento de la maquina Enigma. Turing capitaneaba a un grupo de Hackers durante la segunda Guerra mundial y los Alemanes poseían Enigma. Una maquina de cifrado de mensajes imposibles de entender.

En la actualidad el panorama no es muy distinto. Después de lo que se denomina la «Guerra Fría» parece encenderse una nueva «Guerra Caliente» , se trata de Echelon y Carnívoro. Ambos, sistemas de espionaje parapetrados por el gobierno más poderoso de este planeta.

Echelon consta de una flota de satélites y sistemas de interceptación de ondas electromagnéticas y eléctricas. Detrás de esto, maquinas Crackeadoras de claves, capaces de comprobar millones de claves por segundo, pero apenas conocen el texto en claro. Para ello esta Carnívoro, un Software empleado por el FBI «y quien sabe quien más» capaz de rastrear todos los mensajes que se cruzan por la Red.

Eso si, si le dejan instalar el susodicho Carnívoro, en el servidor. Este «animal» en forma de gran armario repleto de chips y cables, debe de ser instalado conjuntamente con cada servidor de Internet, lo que ha llevado a ciertas incompatibilidades con el Hardware de Carnívoro, menos mal!.

Todo esto demuestra simplemente, que al final algunos «buenos» Crackers se reciclan y prestan sus servicios al Gobierno, o quizás es el gobierno quien les obliga a trabajarpara ellos?. La idea final es la misma, crear un ejercito de Crackers para combatir al enemigo, los Crackers!.

5.3. Recopilación tercera Copiando todo, el Crack de los CD

Cada año se estiman unas perdidas de mas de 300 000 millones de pesetas en el sector del Software, por culpa de las copias piratas de bajo coste que circulan por la red, por otro lado estas perdidas, llevan como consecuencia, el encarecimiento del producto «software» para contrarrestar los gastos de desarrollo del producto, pero lo más grave del asunto, es que si no se revierten los beneficios del mercado del Software, muchos programadores de elite podrían quedarse sin trabajo en breve.

Y es que los programadores y la propia creación de nuevo Software esta en peligro. Con medios no tan elegantes o sofisticados como los que emplean los Crackers, «para reventar un ejecutable» los piratas informáticos son autodidactas que se dedican a duplicar CDs uno tras otro, gracias a la nueva generación de grabadoras de bajo coste. Estos programas duplicados son normalmente versiones que se registran legalmente para obtener el numero de serie del producto. Numero de serie que será empleado para todas las copias del programa realizado.

Sin embargo la amenaza no viene siempre desde el duplicado de un CD. Los Crackers, avezados tozudos de la tecnología logran siempre descompilar los principales ficheros de un programa y leer así todas las líneas de código de programa. La alteración de algunas de estas líneas permite registrar el programa de evaluación sin mayor coste que el consiguiente gasto de energía en el tiempo empleado en modificar la línea de código adecuada. Estos Crackers programan después pequeños programas denominados «Cracks» que se deben ejecutar en el directorio donde se encuentra la extensión EXE principal, consiguiendo añadir un «pacht» en tal fichero, modificando así el registro del programa.

Otros menos expertos, descargan versiones Tryout de las WEB Sites oficiales y modifican los datos de la fecha para alargar la vida de las versiones de prueba. Estaultima opción de emplear un Software bajo el modo «de modificación de fechas» quizás es el modo menos perseguido, dado, que no se realiza copia del programa si no que se trata de alargar la vida operativa del mismo, hasta que un error lo caduca por completo.

Por ello, muchas versiones de evaluación poseen mayores limitaciones que la simple caducidad de la fecha de evaluación, añadiendo por ejemplo un número de usos limitado a 15 o 5 usos. Versiones electrónicas de registro ESD, método que crea ficheros de registro ocultos y que se ubican en la carpeta REG como módulos inamovibles también impiden la modificación de fechas, dado que se trata de una subrutina de control de fechas que detecta si esta es retrasada en el tiempo. Ocurrido esto, el programa se bloquea. Sin embargo no todo es oro lo que reluce, dado que la mayoría de los programas se pueden desproteger si introduces la llave de desbloqueo

del producto, algo bastante fácil para un Cracker, dado que este crea un nuevo miniprograma que obtendrá la clave de desbloqueo a partir de, el numero de serie del producto. «la obtención de este numero de desbloqueo viene siempre definido por un tipo de algoritmo fijo».

También existen otras muchas formas de proteger un programa o software, como por ejemplo «encriptar «ficheros DLL que se ubican en la carpeta Windows/System o emplear llaves electrónicas que deben descifrarse en una llave hardware conectada al puerto paralelo como las empleadas por Hardlook.

Las denominadas llaves Bistro o de Hardlook, son unos pequeños conectores habituados al puerto paralelo de nuestro PC, en el cual lleva integrado un chip ASIC de alta seguridad capaz de generar hasta 43 000 algoritmos de cifrado diferentes. Esta pequeña «placa» puede ser modificada o controlada mediante Software para reprogramarse o recuperar ficheros. Para llevar a cabo estas operaciones se requiere de una placa criptoprogramadora de llaves, la cual nos llega con un único código elegido al azar, esto es, ninguna otra placa criptoprogramadora tendrá la misma llave de acceso. Este nuevo método para proteger nuestros datos mediante sistemas basados en Hardware es probablemente uno de los sistemas mas seguros a la hora de proteger nuestro software o ficheros, dado que por citar un ejemplo, tenemos que hemos creado un Software y queremos distribuirlo, pero antes, alguien interesado en nuestro Software nos pide una copia para estudiarlo.

Para evitar que esa copia «estamos pensando lo peor» sea duplicada y falsificada, podemos generar una llave de bloqueo en el arranque del programa, esto es, en elfichero EXE principal. Tras para lo cual se necesitara de la llave «hardware» para arrancar el programa. Esta llave la programamos nosotros y la añadimos al producto.

Este tipo de defensa nos permite controlar el numero de copias de nuestro Software y supera con creces la protección mediante Software como el de registro de ficheros de entrada, el cual puede ser «saltado» perfectamente «congelando» la fecha del ordenador. La guinda del pastel, la ofrecería la posibilidad de adaptar estas llaves con un segundo algoritmo temporal para muestras de evaluación sin necesidad de llave física, para evitar el falseamiento de esta, algo casi imposible por tratarse de un ASIC.

Otra de las características que destacan este tipo de protección mediante Hardware, es la posibilidad de direccionar el chip en al menos 30 direcciones aleatorias, esto complica aun más las cosas, dado que el Hacker debería, para romper el cifrado, adivinar en que registro esta la llave correcta.

Por otro lado si un Hacker logra «robarnos» un fichero importante de nuestro disco duro, este seria inservible sin la llave física, única y que esta en nuestro ordenador, mas concretamente en el puerto paralelo de nuestra maquina. Es pues, este, un sistema altamente seguro de protección de software. Todo lo descrito hasta

aquí, sencillamente nos muestra como están las cosas en el mundo del Software de PC, digamos que es una batida continua por ver quien es más rápido en romper una protección. Sin embargo el interés principal de la comunidad Hacker no esta en precisamente romper la fecha de caducidad del programa, mas bien el interés esta en como copiar un CD protegido contra copia.

Esto es así, ya que sin ir mas lejos, la Playstation emplea CD como soporte para sus videjuegos. Este mercado tan poderoso y la proliferación de grabadoras para PC, son la combinación perfecta para la comunidad Hacker. Así que dejando a un lado los métodos de protección de un ejecutable, pasemos a revelar los mejores Cracks de Cds protegidos.

5.4. Recopilación cuarta El Crack de la Playstation y Dreamcast

En la actualidad ya son muchos, los Cracks disponibles para la consola de Playstation y en definitiva están para eso, para crear un Crack en el interior de la consola. Lamentablemente, este es el aspecto de toda esta historia.

La historia del Crack de Playstation se inicia cuando Scott Rider de REI «Reverse Engineering, Inc» escribe un código para «paliar» el problema del código regional. La idea era conseguir que una consola fabricada para el mercado Asiático, Americano o Europeo, fuera capaz de leer un disco fabricado para otra región que no fuera el suyo. La idea funcionó bastante bien, Scott Rider instalo el chip en la consola Playstation y comprobó que todo marchaba según lo previsto.

El efecto secundario fue, que el «Modchip» a la vez que eliminaba la limitación del uso de un juego distribuido en USA por una consola fabricada para Europa, también quitaba la protección anticopia. Esto fue bien recibido por la comunidad Hacker, mientras que a Scott Rider le quedaba una espina clavada en el estomago, por lo que parece que no le sentó nada bien el asunto. Prueba de ello es que después Scott Rider escribió un nuevo código el cual, permite el intercambio de juegos entre continentes, pero que restauraba la protección de nuevo.

Sin embargo este no era el fin del Crack de Playstation, ya que lo comunidad Hacker distaba mucho de mantener el código de Scott Rider. Prueba de ello es que en la actualidad ya existen diferentes y variados códigos reescritos que no restauran

precisamente el sistema de protección. Los Modchip, permiten ahora incluso activar el color de un videojuego fabricado para el mercado NTSC, en el momento que se esta reproduciendo en un televisor PAL.

Pero para los que no les entusiasma la idea de desmontar su consola y soldar un Modchip en su interior, tienen otra alternativa de jugar con los CD destinados a la Playstation. Se trata de Bleem, un sofisticado emulador del Hardware de la consola Playstation, que corre bajo el modo de Software en un simple PC. Este programa nace hace ahora apenas un año y medio y ya esta causando estragos, incluso en los directivos de Sony que han visto como perdían una primera batalla en los tribunales contra los creadores de Bleem.

Claro que todo esto es un poco complicado de comprender ahora mismo. De modo que vayamos por pasos.

5.4.1. Un poco de historia, el principio

Cuando se fabricó la PlayStation y sabiendo que un CD sería fácilmente duplicable en un futuro próximo, se crearon una serie de protecciones con el fin de poner el máximo de trabas al mercado negro. Entre estas protecciones está la de la detección del color del disco, (los famosos CD's negros de PlayStation), aunque esta protección no es muy efectiva contra los nuevos CD's verdes o azul oscuro. También los CD's de PlayStation poseen unas pistas que contienen información de la región del mundo para la que se ha licenciado el juego y solamente podrán ser usados por consolas pertenecientes a esa región. De esta forma un CD comprado en USA o Japón no funcionará en una consola europea. Para colmo estas pistas están grabadas en el CD con los EDC/ECC a cero, esto es, cuando una pista se graba en un CD, al final de la pista se escribe una especie de suma de la información que contiene con el fin de detectar y corregir posibles errores (EDC/ECC), pues bien, los EDC/ECC de estas pistas están a cero aunque contienen información. Esto sólo se puede hacer con grabadoras especialmente diseñadas para esto. Cualquier grabadora convencional, al escribir estas pistas pondrá automáticamente los EDC/ECC correctos a la información que poseen las pistas. Esto es inevitable y en la actualidad no reproducible, por lo tanto la consola detecta a través del EDC/ECC de estas pistas si el CD es original y por la información que contienen si es de la región de la consola.

Aquí es donde entra en juego el chip MOD, éste chip no se sustituye por uno de la consola, sino que se añade a esta, este chip se encarga de que cuando insertamos un CD copiado o de otra región en la consola, interceptar la información de las pistas de protección del CD y mandar a la consola la información correcta que esta espera, como que es un disco original y que la región es la de nuestra consola. Una vez hecha la comprobación, el CD se ejecutará normalmente y no se repetirá esta comprobación hasta que cambiemos de CD o abramos y cerremos la tapa del lector de la consola.

5.4.2. Modchip, el Crack de la Playstation

Normalmente, el chip empleado es un PIC12C508 de Microchip Technoloy Inc., importado en España por Sagitrón. Se trata de un circuito integrado de ocho patillas que a grandes rasgos contiene un microcontrolador de 8 bits que entiende unas 33 instrucciones, una memoria RAM para poder ejecutar el programa y una memoria PROM que lo almacena. Cuando compramos el chip en la tienda (entre 200 y 400pesetas), la memoria PROM esta vacía, por lo tanto el microcontrolador no tendrá instrucciones para ejecutar y el chip será inútil. Para que el chip sea operativo debemos colocar un código con instrucciones en la memoria PROM, para ello debemos emplear un programa y un programador. El Modchip que es así, como se le conoce en la jerga de la ReD, puede estar disponible para su instalación en dos modos bien distintos, una vez que se ha programado correctamente. Ambos modos responden a códigos diferentes, así un código implicara el utilizar 4 pines del chip y otro código, implicara el utilizar 5 pines.

La diferencia más notable de ambos modos, es que la versión de 5 pines utiliza el reloj de sincronismo de la propia consola, mientras que la versión e 4 pines, utiliza el reloj interno del Chip. En la practica esto implica que el código que utiliza 5 pines del Chip es el mas adecuado para instalar en la consola, según se desprende de varios mensajes localizados en la ReD. El porque, tiene una explicación sencilla y es que si se emplea la frecuencia de reloj interna del chip, dicha frecuencia varia en función de la temperatura. Esto implica que muchas veces la consola genere un error de lectura de la secuencia Boot de arranque del disco.

5.4.3. El Crack de la Dreamcast

Tambien aqui se puede hablar del Modchip, pero mas elegante es presentar un nuevo Crack de reciente descubrimiento. Se trata de de utilizar la Dreamcast como lector de discos «dado que un disco de la Dreamcast posee 1GB de capacidad» y el PC como conversor de datos, para despues integrarlo todo en un CD estandar.

Entre la Dreamcast y el PC, un avanzado Hardware de fabricacion casera, capaz de filtrar los datos correctos. Los esquemas y el Software estan disponibles en Internet, pero se avisa, no es apto para cardiacos.

5.5. Recopilación quinta Cracks, desprotegiendo el Software

Para desproteger el Software, hace falta aplicar la ingeniería inversa en ellos, pero esto es algo que no esta al alcance de todos. De modo que los Crackers ponen a disposición de los internautas pequeñas aplicaciones fruto de la ingeniería inversa y que cualquiera podrá aplicar sin grandes conocimientos. Estas pequeñas aplicaciones capaces de «aplicar» la ingeniería inversa a un Software se llaman Cracks. Estos Cracks suelen funcionar de diversas formas.

5.5.1. El Patch o Crack por Software

Para crear los Patch, los Crackers normalmente descompilan el ejecutable principal y tras localizar la línea de código que necesita, escriben un pequeño programa Parcheador. Este tipo de Cracks se basa en ejecutar el parcheador en el mismo directorio donde esta ubicado el programa a Crackear. Todo este proceso implica dos delitos al mismo tiempo. El Cracker comete delito cuando hace uso de la

Ingeniería inversa para parchear la línea de código oportuna y el usuario comete un segundo delito, cuando ejecuta y parchea el programa que requiere licencia.

Este tipo de Crack es el mas devastador de todos y el que implica un grave delito de aplicación de Ingeniería inversa por parte de todos los que lo emplean. Otros Cracks se basan en un generador del numero de serie del programa a partir de un nombre de usuario.

Se trata de un pequeño programa que genera el numero de serie después de escribir en el, un nombre de usuario. El Cracker ha obtenido el algoritmo correcto, después de aplicar la fuerza bruta en un programa registrado legalmente. En este sentido se entiende que un Cracker puede adquirir legalmente una copia del Software a «reventar». Estos Cracks son menos agresivos y en una primera visión, carecen del empleo de la Ingeniería inversa.

Finalmente, podemos encontrar el Crack del registro. Este Crack es muy simple y no suele estar creado por un Cracker, sino por cualquiera que utilice un ordenador. Se trata de crear un fichero con extensión *.nfo, en el cual se escribe el nombre de usuario y el número de registro del programa afectado. Estos datos se obtienen de un programa legalmente registrado, así que esto mas bien podría ser una difusión de la licencia, mas que un Crack. Este acto también esta penalizado por la ley.

5.5.2. Appz

Básicamente, los Appz son programas completos con parcheador incluido, que se pueden descargar desde sitios ftp. Este tipo de sites están constantemente perseguidos por la BSA, por lo que es normal ver como desaparecen con cierta facilidad de la ReD.

El delito en este sentido es muy grave, ya que se violan los derechos de autor y se aplica ingeniería inversa si el programa descargado contiene un parcheador.

Los Appz no responden a perfiles de Crackers, ya que un Appz lo puede colocar en la ReD cualquier internauta. Se trata simplemente de colgar un archivo en la ReD.

5.5.3. SerialZ

Los SerialZ son simplemente paginas HTML que contienen todos los números de serie de los programas mas conocidos. Esto no es un Crack, sino una difusión de datos de alguna manera protegidos. Aquí tampoco interviene un Cracker.

5.5.4. WareZ

Los WareZ son idénticos a los Appz. Se trata de paginas Web, desde donde se pueden descargar programas completos. La única diferencia entre los Warez y los Appz esta, en que los primeros son programas con registros idénticos en todos ellos. Esto es, que no se aplican parcheadores y en su lugar, se añaden los SerialZ.

5.6. Recopilación sexta Phreakers, Crackeando el teléfono

Phreakers, una extensión mas del Underground y descendientes directo de los Hackers y Crackers, pretenden conocer a fondo la tecnología y los entresijos que encierran la telefonía fija o móvil. Altamente penado por la ley, las soluciones que se adoptan para «manejar» esta tecnología a su antojo, esta exquisitamente guardada y los Phreakers abundan por su reducido grupo de maestros en el arte.

Kevin Mitnik, el mayor ejemplo «a seguir» a sido uno de los últimos Phreakers en dar con sus huesos en la cárcel, por un delito múltiple de Crackeo de equipos telefónicos y por el robo de importantes programas de desarrollo de teléfonos móviles, los cuales no se van a citar aquí, pero si sus heroicidades.

Tron, amigo nuestro y miembro del Computer Chaos Club, ya no esta entre nosotros para contarnos como se hizo con las «claves» de la telefonía móvil. Una

desaparición primero, y una muerte injusta después, han hecho que nuestro amigo nos diga adiós para siempre injustamente.

Otros con mas suerte como el Capitán Crunch siguen vivos y pueden contarnos sus hazañas. El capitán Crunch, conocido así por una conocida marca de cereales, fue el primer Phreaker que se conoce. Sus tácticas, tan curiosas como emplear un silbato «que regalaba una marca de cereales» han sido el principio de las famosas «cajas de color» de las que tantos y tantos «usuarios» han empleado para llamar gratis por teléfono.

Ahora los Phreakers no se dan a conocer, pero están todavía ahí, y más fuertes que nunca. Burlando las leyes de la física y la tecnología, presentan en sus reducidos «eventos» sofisticados sistemas informáticos y electrónicos capaz de burlar incluso a los satélites de comunicaciones. Las claves y los secretos en este reportaje.

5.6.1. Haciendo Phreaking

Uno de los casos más curiosos esta protagonizado por el Capitán Crunch, percusor de este «arte» de engañar a los teléfonos, cuando por una de las casualidades de la vida, descubrió que mientras hablaba por teléfono con una amiga, este se quedaba en silencio, cuando de forma arbitraria silbaba con un silbato que había obtenido como regalo de los cereales Capitán Crunch, de ahí el nombre de este personaje hecho esto observo, que la línea enmudecía cada vez que silbaba, lo que motivo en una investigación por parte del Capitán Crunch.

Lo que sucedía es que la línea se «cortaba» es decir, había emulado el pitido que indica la central de que se ha colgado el teléfono, pero el no lo había colgado, porque estaba hablando todavía, con lo cual la línea estaba abierta y el contador no marcaba los pasos por creer que el usuario había colgado. Ahora solo quedaba por determinar a que frecuencia «silbaba» el silbato y resulto ser a 2.600 Hz. De esta forma el Capitán Crunch se construyo un oscilador electrónico a dicha frecuencia, y lo dio a conocer entre la comunidad Hacker. Dicho invento recibió el nombre de Caja azul, dado hecho porque Pacific Bell intervino multitud de estas cajitas en una redada y todas eran azules.

5.6.2. Tron, amigo ya no estas entre nosotros

Este es un caso difícil de explicar, por lo que no entraremos en complicados detalles, pero quizás es el caso de Phreaking más «oscuro» de la historia, pero vale la pena recordarla, en memoria de nuestro amigo Tron.

El 24 de Octubre de 1998, un miembro de CCC «Computer Chaos Club» llamado Tron es víctima de un homicidio. Su cuerpo fue hallado en el interior del parque de Neukölln, Berlín, Alemania. Las fuentes policiales dictaminaron que había sido un suicidio, sin embargo los miembros de CCC no son de la misma opinión. Tron fue una de las más brillantes cabezas dentro de las filas de Hackers de Europa.

Tron era capaz de fabricar tarjetas prepago de teléfonos públicos, siendo así, el primero en crear las maravillosas tarjetas mágicas, lo que puso en guardia a la principal compañía de telefonía en Alemania.

Tras esta experiencia, Tron contacta con CCC y ofrece sus conocimientos técnicos, explorando todas las tecnologías, Tron inicia un largo camino en el estudio de la criptografía. Algo que le vale para entender el algoritmo de la telefonía celular y las tarjetas SIM. A partir de este momento Tron es capaz de «clonar» con éxito las tarjetas GSM, así como entender a fondo los sistemas ISDN.

Sin embargo tales conocimientos quedan al alcance de pocos, ya que Tron desaparece trágicamente. Con un carácter abierto y alegre, es difícil entender como Tron optaba por suicidarse. Dos meses después de su «muerte» la prensa informa al mundo que por fin «un ingeniero de telefonía» ha sido capaz de descifrar el contenido de cientos de cintasgrabadas en el reinado de Hitler. Es acaso esto una coincidencia. Todas las sospechas están abiertas.

5.6.3. Crackeando el satélite

El día 28 de Febrero de este mismo año, saltaba la alarma de nuevo en el mundo de la seguridad. La agencia de noticias Reuters se daba eco de una noticia mas que preocupante. Según Reuters alguien había conseguido hacerse con el control de un satélite militar espía Británico y para mas inri lo había desviado de su órbita regular.

El satélite al que se hacia mención, era uno de los encargados de repeler un ataque nuclear y formaba parte de un grupo de 4 satélites denominados Skynet. Estos

satélites se emplean para el control de los conflictos dentro de Europa como el ocurrido recientemente en los Balcanes. El posible satélite controlado por los hackers sería el denominado 4D, lanzado el 10 de enero de 1998 en un cohete tipo Delta 2.

En el espacio existen unos 300 satélites de este tipo. Dichos satélites poseen multitud de canales de comunicación secreta para entornos militares. Dichas comunicaciones son el eje en un conflicto y afecta directamente en el resultado de este. Por ello los Hackers «Phreakers» parecen tener el ojo puesto en este prometedor método de comunicación, dando un paso mas allá que el simple teléfono.

5.6.4. Virus en los teléfonos móviles, mito o realidad

Hace unos meses salto de nuevo la alarma mas temida, la existencia de un nuevo virus malicioso, pero en este caso la noticia cobraba mas interés, dado que el nuevo virus anunciado era enviado a través de la red GSM de todo el país hasta alcanzar un numero concreto de teléfonos móviles.

La noticia matizaba con especial interés que el nuevo virus era capaz de borrar o modificar la ROM del teléfono celular, de esta forma el teléfono quedaba inservible. Pero la buena suerte parece correr de nuestro lado, ya que hasta el momento no hemos conocido a nadie que haya perdido su teléfono celular por estas circunstancias.

5.6.5. Wap, la llegada de las pesadillas de la ReD

Sin entrar en detalles de lo que es el WAP, en estas líneas solo queremos hacer constancia de una «predicción informática» y es que la nueva solución de WAP, que parece querer introducir Applets de Java, Gifs y otros ficheros de la ReD, podrían ser lacausa de la existencia de nuevos virus informáticos, diseñados en este caso para los teléfonos celulares que soporten la nueva generación de WAP. Si no, tiempo al

tiempo.

5.6.6. Phreakers en el gobierno

Con los nombres claves de Echelon, Enfopol y Clipper Chip, parece ser que existen mas casos de Phreaking en los altos cargos del gobierno que fuera de ella. Nos referimos a que las escuchas telefónicas no son del todo legales hasta que las solicita un juez, y aun así se atenta contra la intimidad de cada uno.

Echelon, Enfopol o el Clipper Chip es en resumidas cuentas un ejemplo del Phreaking al mas alto nivel, ya que emplean métodos poco ortodoxos para interceptar las comunicaciones de teléfono. Por ejemplo el Clipper Chip emplea una puerta trasera para desencriptar la comunicación interceptada. Esto es, que emplea un algoritmo de cifrado de datos vulnerable y al servicio de la CIA.

Mientras tanto los sistemas de Echelon o Enfopol, emplean la intercepcion de líneas y ondas hertzianas para conseguir el mismo efecto, de esta nueva forma de hacer Phreaking hablaremos en el siguiente bloque.

5.6.7. Echelon, un caso de Phreaking al por mayor

Hace 40 años Nueva Zelanda creo un servicio de inteligencia llamado GCSB «Government Communications Security Bureau» el equivalente a la NSA americana. Ahora y en colaboración con la NSA, crean Echelon. Un avanzado sistema de espionaje a escala mundial, que junto con UKUSA y el empleo de Satélites Intelsat, las nuevas inteligencias gubernamentales pueden desde hace tiempo acceder e interceptar todas las comunicaciones tradicionales como el teléfono, el fax o el correo electrónico.

Desde 1996 Nicky Hagar›s nos muestra otro tipo de espionaje secreto, descubierto

en su libro Secret Power, Nicky revela que estamos siendo espiados en todo momento.

Según su libro, Nicky afirma que lo que estoy escribiendo ahora es susceptible de ser espiado incluso en el borrador desde mi PC, mediante el método TEMPEST. Este sistema de espionaje aprovecha la radiación electromagnética de la pantalla de mi monitor para recibir todo lo que se muestra en mi monitor. Por otro lado cuando termineeste articulo y lo envíe por el correo electrónico, este será inmediatamente interceptado por la estructura Echelon y por supuesto analizado.

Por otro lado si envío un fax a mi editor o le llamo telefónicamente para confirmar que ha recibido el articulo, Echelon también dispondrá de una copia del fax y de la conversación telefónica. Pensar en todo esto, simplemente le pone a uno los pelos de punta.

En 1948 se formaliza UKUSA después de interceptar varias comunicaciones de radio secretas durante la segunda guerra mundial. Junto con Echelon, UKUSA «denominada Spy Network» potencia las posibilidades de controlar las comunicaciones globales desde los satélites Intelsat.

El jueves, 12 de junio de 1984, Rob Muldoon conviene en el parlamento lo que seria el primer paso para crear Echelon. Diez años mas tarde, el 15 de enero de 1994 los técnicos de satélites interceptan comunicaciones extrañas en los satélites, fecha en la que se revela la existencia de UKUSA.

Desde entonces todas las comunicaciones son interceptadas por Echelon y Ukusa y descifradas por técnicos expertos en busca de información confidencial de un posible movimiento militar, terrorista o de otra índole.

Las principales formas de espionaje se basan en interceptar las comunicaciones por radio sea cual sea su banda. Pero las potentes cámaras de vídeo de ultima generación y las nuevas lentes ópticas, permiten obtener imágenes sorprendentes desde una distancia mas que alarmante comprendida en varios cientos de kilómetros de distancia.

Esta técnica, se sobreimpone a la captacion de ondas de radio. Por otro lado Internet, el gran complejo de comunicaciones digitales mundial también esta siendo espiado por la nueva inteligencia gubernamental. Otro peligro sé sobreimpone por el empleo de teléfonos móviles. Todos los datos «pinchados» se codifican y se envían al espacio hacia los satélites donde sé multiplexan todas las señales para ser distribuidas hacia los centros de computación y control.

Estas bases terrestres además de recibir toda la información están diseñadas para «escanear» y recibir todas las frecuencias de los satélites en busca de información conflictiva. En los centros de control de estas bases tiene lugar el estudio de todas las señales «interceptadas» entre las cuales pueden existir informaciones en claro e informaciones encriptadas.

Las informaciones en claro se entienden por todas aquellas que están codificadas bajo cualquier estándar analógico o digital, pero que los ingenieros conocen perfectamente. Las señales encriptadas son aquellas que se basan en contenidos cifrados imposibles de descifrar sin la clave adecuada.

Estos últimos mensajes son quizás los que más preocupaciones causa dentro de la red «de espionaje mundial» ya que a menudo no se pueden obtener los mensajes en claro aun empleando métodos de «descifrado» de señales.

Por ello, quizás quede alguna esperanza por mantener la privacidad aunque no la intimidad de nuestras comunicaciones y es empleando sistemas criptográficos para la voz y el correo electrónico.

5.7. Recopilación septima Hackers en el poder, Phreakers en el gobierno y 2

Bill Gates y Paul Allen, trasteaban con los primeros Microprocesadores de Intel allá por el año 1972. El microprocesador en cuestión era el modelo 8008, y en aquel momento la industria informática no tenia en consideración la posibilidad de construir una computadora personal, basado en este procesador. Sin embargo Bill Gates y Paul Allen sentían que su momento estaba cada vez mas cerca. Tres años mas tarde, en 1975 Intel saca un nuevo procesador con mas de 10 000 transistores y bill Gates junto con su amigo, desarrollan el primer software para Altair. Este es el primer paso, mas adelante trabajan con lo que hoy conocemos como MS-DOS. Ambos jóvenes, todavía no muy conocidos, son denominados Hackers. Pero estos jóvenes han crecido y a su alrededor ha crecido todo un imperio llamado Microsoft, esta es la parte buena, la parte mala, es la que sigue.

Con los nombres claves de Echelon, Enfopol y Clipper Chip, parece ser que existen mas casos de Phreaking en los altos cargos del gobierno que fuera de ella. Nos referimos a que las escuchas telefónicas no son del todo legales hasta que las solicita un juez, y aun así se atenta contra la intimidad de cada uno.

Echelon, Enfopol o el Clipper Chip son en resumidas cuentas un ejemplo del Phreaking al mas alto nivel, ya que emplean métodos poco ortodoxos para interceptar las comunicaciones de teléfono. Por ejemplo el Clipper Chip emplea una puerta traserapara desencriptar la comunicación interceptada. Esto es, que emplea un

algoritmo de cifrado de datos vulnerable y al servicio de la CIA.

Mientras tanto los sistemas de Echelon o Enfopol, emplean la intercepcion de líneas y ondas hertzianas para conseguir el mismo efecto. Acaso no es esto un acto de Phreaking?. Soro, un Phreaker español expone su opinión al respecto.

…Parece inevitable el catalogarnos a nosotros, como los únicos malos. Si yo consigo crear un clon de una tarjeta prepago de teléfono, soy un delincuente, si consigo realizar una escucha en una línea de teléfono de mi vecino, soy un delincuente, si Echelon escucha a medio mundo interceptando correo electrónico, Fax y teléfono, es simplemente para realizar su trabajo. Que sucede realmente?. Porque un Hacker o un Phreaker es solo malo cuando esta fuera del gobierno?.

Soro se muestra escéptico sobre esto, cree a su vez que los Hackers, los Crackers y los Phreakers ocuparan al final, un lugar dentro de las esferas mas altas de cada estado, como parte del personal cualificado.

…Es inevitable. Internet es mas que una revolución para la sociedad. Internet es la puerta para el Hacker, el Cracker o el Phreaker. Que ordenador no esta ya conectado a la ReD?. Cada día se rompen mas cortafuegos, se crean mas virus y se desarrolla mas Software para romper sistemas, en definitiva, cada día hay mas gente que domina el arte del Hacking, pero cuidado, también es cierto que cada día hay mas gente que emplea mal las técnicas del Hacking o para fines nada correctos. Por esa misma razón, los gobiernos de todos los países, deben aceptar a buenos Hackers, …de Fiar… -Sonríe- …para contrarrestar las hazañas de algunos buenos hombres malos. Dicho esto, no queda mas que decir.

5.8. Recopilación octava Hackers, la rebelión de algunos hombres buenos.

En el argot informático, Hacker es aquel con amplios conocimientos informáticos, capaz de pasearse a sus anchas por los discos duros remotos vulnerando todo tipo de puertas de seguridad, haciendo uso de los Bugs informáticos. Fallos, que nunca sabremos si están en los sistemas por cuestiones técnicas, por error o simplemente porque los programadores lo han dispuesto así y punto.

Tal es el interés, creado en torno a los Hackers, que tanto el cine como la literatura recurren a ellos de forma menuda. Solo hay que echar una mirada a nuestro

alrededor para comprender lo que esta sucediendo. Bruce Sterling, Anonymous o John Markof son los nombres habituales que podemos encontrar en las librerías. Pero el tema de los Hackers ya no les pertenece solo a ellos.

En nuestro País, Arturo Pérez Reverte muestra su interés por los Hackers en su novela La piel del tambor. La novela arranca con la intrusión de un Hacker en los ordenadores del Vaticano, el padre Ignacio Arregui, un jesuita huesudo y flaco será el soldado que deberá defender las redes del Vaticano en el resto de la novela, con la ayuda de otros Jesuitas expertos informáticos.

Arturo Pérez Reverte cree que los Hackers se retuercen de placer, cuando consiguen penetrar en el sistema del chase Manhattan Bank, el Pentágono o el vaticano. Y en parte tiene razón, de modo que los define de una forma muy curiosa, les llama los yonquis del chip. Mas adelante hace mención en otro punto importante en el mundillo de los Hackers y los Sysops.

El padre Arregui pone el dedo sobre el cursor que en ese momento parpadeaba en rojo e inquiere, ¿ Es nuestro Hacker?, a lo que el otro Jesuita responde que si, ¿ Que nombre le ha asignado? añade el padre Arregui, Vísperas, responde el Jesuita, Vísperas. Es por lo único que se les conoce, por el Nick. Su rostro se representa por un Nick, su imagen es un Nick y el propio Nick tiene un significado, así como refleja la personalidad del Hacker. Ahora Vísperas había entrado en el ordenador personal del Santo Padre.

5.8.1. El primer Hacker

Ahhhhjaja, quien fue primero, que Nick tenia o eso fue mucho después cuando llego todo eso de los cambios sociales e ideológicos. Quien se proclamó a los cuatro vientos soy un Hacker. Se han escrito muchas buenas historias. Podemos ordenarlas por fechas,pero las conocemos todas?. Ni siquiera los escritores que se pasan la vida recopilando información sobre el tema, pueden concretar una fecha, una hazaña o un principio concreto. Acaso es posible crear una línea divisoria entre el Hacker y el curios?. En 1959 cuando las computadoras eran enormes masas de cables, válvulas y más masa de cables, un grupo de alumnos del prestigioso Massachusetts Institute of Technology «MIT» protagonizaron lo que para algunos seria el primer acto de Hacking informático. La afirmación esta fundamentada, ya que en aquella época, la

época de los dinosaurios metálicos, solo los operadores tenían acceso a estas moles y solo sus dedos podían acariciar las tarjetas perforadas.

Lo que creaba directamente una sensación de deseo a los usuarios que debían entregarles los programas a los operadores, para que estos, mas tarde y tras introducirlo en el ordenador, les devolviese los resultados. A los chicos del TMRC miembros del Club de modelo de trenes esto les ponía, francamente malos, de modo que se las ingeniaron para introducir ellos mismos «en ocasiones aisladas» los programas en el ordenador. Pero seguía sin ser suficiente y se las ingeniaron de nuevo, para esta vez, tener contacto con el ordenador desde una sala de terminales a la que en realidad no tenían acceso de forma oficial, colándose en ellas por las noches, sin preocuparles las menudencias administrativas.

Poco tiempo después uno de los alumnos aventajados, llegaba a ser un destacado profesor del MIT y en aquel entonces aparecía un nuevo ordenador mucho mas avanzado, el TX-0, que introducía el teclado. Esto les permitía introducir directamente los datos en el ordenador y obtener los resultados de forma directa. Esto les motivo profundamente y la respuesta estaba en pasar largas horas delante del ordenador, lo que les llevo a realizar cosas con el ordenador que ni los propios diseñadores podían imaginar.

Fue en ese entorno cuando el termino Hacker comenzó a aplicarse a aquellos pirados de la informática que se pasaban largas horas delante del ordenador y hacían cosas con ellos que se salía de ciertos cánones. En cualquier caso el bautismo de fuego no fue precisamente, el adoptar el termino Hacker, sino de ser los primeros en pensar de forma diferente acerca de como utilizar los ordenadores y que se podía hacer con ellos. Las posibilidades debieron de ser muchas para que estos estudiantes crearan una ética que regia el comportamiento de los Hackers. Esta ética aun a día de hoy, esta vigente y parece ser respetada y comprendida por todos, por lo menos cuando se trata dereivindicar que la información debe ser libre para todos. Esta forma de ver las cosas, es probablemente el pilar de todos los Hackers.

Pero ahora viene la pregunta del millón, son estos estudiantes del Tech Model Railroad Club, los primeros Hackers de la historia?. En parte podría decirse que si, ya que la fecha en la que suceden los hechos juega un importante papel. Estamos hablando de cuando los ordenadores se llamaban computadoras y carecían de teclado.

Sin embargo queda reflexionar un poco. La palabra Hacker esta atribuido a los que tocan los ordenadores y al mismo tiempo se les atribuye este nombre a los curiosos, a los que estudian los sistemas, a los que quieren saberlo todo acerca de lo que tiene delante o puede tocar. Entonces quien no afirmaría que antes que estos muchachos, otros, ya pretendían desvelar todos los misterios de los avances tecnológicos de aquel entonces.

Un técnico debe conocer a fondo el sistema eléctrico, electrónico o mecánico, si

quiere dar con la avería y repararla. En parte los técnicos son los mas interesados en conocer el sistema. Para ellos la información debe ser libre, a cuanta más información, mayor eficacia en su trabajo y más rentabilidad. Además solo una fuerza mayor les ha motivado a ser técnicos. Por que les gusta.

Entonces, como sabemos quien fue primero?. Dada la situación tomemos como los primeros, a los chicos del TMRC y el MIT, solo por el hecho de ser los primeros en adoptar el termino Hacker.

5.9. Recopilación novena Hackers de 15 años

Cuando se habla de Hackers siempre se nos viene a la cabeza la imagen viva de unos chalados por los ordenadores, melenudos y a menudo rodeados de latas de coca-cola, mientras sus cuerpos están encorvados sobre el teclado en medio de la noche. Nada mas lejos de la realidad, los Hackers de hoy, apenas son unos adolescentes de 15 años que muestran su habilidad haciendo frente a los sistemas de seguridad más grandes del mundo. El Crack del sistema de discos DVD o el reciente ataque masivo a varias paginas comerciales en Internet, han sido, solo algunos de los ejemplos recogidos en los últimos días en toda la prensa mundial. Un grupo de Hackers a descifrado el código CSS del sistema de disco DVD, un grupo de Hackers mantiene al FBI en jaque en los recientes ataques en Internet…son algunos de los titulares a los que ya estará acostumbrado, pero es evidente que solo nos deja ver parte de la historia, pero no toda.

En cierta manera puede resultar interesante conocer este tipo de noticias, en un momento en el que toda la informática gira en torno a la seguridad, los virus, los ciberdelincuentes de la ReD y por supuesto los Hackers. Pero lo que más nos llama la atención a todos es quizás la corta edad que presumen tener los nuevos genios de la informática, es decir, los nuevos Hackers.

Después de una exhausta investigación sobre los últimos acontecimientos en el mundo Underground, hemos descubierto que los mayores ataques contra la seguridad y la tecnología, es decir las mayores roturas de sistemas, han sido capitaneadas por jóvenes adolescentes que apenas si han cumplido los 15 años.

Siguiendo el perfil de Bill Gates, los nuevos manitas de los ordenadores ya son capaces de desmontar toda una tecnología que miles de ingenieros han creado a lo

largo de muchos meses de trabajo, en tan solo unas pocas horas. Evidentemente se trata de genios, adolescentes de 15 años que apenas han aprobado EGB, pero que sienten una cierta pasión e interés por los ordenadores y todo lo que le rodea. Son los nuevos Hackers, son la nueva emulación del joven Bill Gates cuando entre las cuatro paredes de un garaje trataba de desmembrar el primer procesador de Intel o acaso muchos de vosotros desconocíais que Bill Gates era un Hacker en su bien temprana edad.

5.9.1. Con 15 años rompe el sistema de cifrado del DVD

La debilidad del algoritmo de encriptación de los discos DVD, «40 Bits» ha permitido a un grupo de Hackers Noruego «MoRE, Masters of Reverse Engineering», entre los que destaca Jon Johansen, un estudiante de 15 años, a descubrir que en su ordenador, el sistema de protección del DVD podía «romperse» con un programa pequeño y relativamente simple que creó en unas pocas horas.

El DeCSS permite volcar el contenido de un DVD al disco duro de un ordenador y reproducir la película con calidad perfecta. También, este pequeño programa permitecrear un duplicado desprotegido del contenido DVD en un disco virgen por medio de una Grabadora, con la misma facilidad con la que hacemos una copia de archivos.

A las pocas semanas de aparecer DeCSS en la ReD, se decide retrasar el lanzamiento del DVD-audio, dado que se cree conveniente introducir un nuevo nivel de protección mucho mas potente, que permita al mismo tiempo dejar obsoleto al DeCSS. Se presenta así, CSS2, un algoritmo más complejo que el endeble CSS «Content Scrambling Systems», sin embargo creemos fervientemente que CSS2 dejara de ser seguro muy pronto

5.9.2. A los 10 años descubre que puede llamar gratis por teléfono

Es quizás, y con toda probabilidad el Hacker mas joven hasta el momento. Se trata de Tim Rosenbaum, un chico que a la temprana edad de 10 años, acometió, lo que hasta la fecha será la mayor estrategia lograda.

El buen chico nació ciego, pero dios le dio un excelente sentido, el oído, con una sensibilidad superior a los demás seres mortales. Sus blandas yemas de los dedos también poseían un tacto inverosímil, capaz de almacenar el tacto suave o áspero de las cosas y reconocerlas por ellas después.

Y también tenia algo que fascinaba a todos los chicos de Dollan, un pequeño pueblo costero al este de Maine, y esto eran sus silbidos. Era capaz de imitar a los pájaros de todas las clases y sobre todo podía controlar el tono del silbido hasta alcanzar notas musicales, hasta que un buen día le sucedió algo realmente importante.

A Tim le encantaban los teléfonos y sobre todo le encantaba escuchar la voz del otro lado del hilo cuando alguien llamaba a casa. Cada vez que podía marcaba un numero cualquiera de teléfono y se sentaba a escuchar la cálida voz que decía; Este numero esta fuera de servicio.

Hasta que un buen día Tim silbó al tiempo que la voz decía la frase y callo de golpe. Esto asombro a Tim. Volvió a marcar otro numero de teléfono, silbó y sucedió lo mismo. Años mas tarde descubría que era capaz de generar silbidos a una frecuencia perfecta de 2.600 ciclos, el tono que indica que el teléfono esta colgado.

5.9.3. Los ataques de negación DoS y MafiaBoy, más adolescentes de 15 años

Durante varios días MafiaBoy a encabezado el mayor ataque de Internet conocido hasta el momento. El FBI y los mejores Hackers del país han estado en jaque durante los días 7, 8 y 9 de Febrero del presente año y el resto de los días hasta hoy. El motivo, un bloqueo masivo de las páginas más importantes de EE.UU. es decir, eBay, Amazon, CNN, Buy.com o Yahoo entre otros.

Pero MafiaBoy es el Nick de un joven Canadiense de 15 años, de modo que tuvo que comparecer, tras ser detenido el 15 de Abril, por un tribunal de menores que lo

dejo en libertad bajo fianza unas horas después. Eso si, se le impuso severas limitaciones como por ejemplo que no puede utilizar un ordenador excepto el del Colegio y bajo supervisión de un profesor o de no poder entrar en una tienda de informática o recintos donde haya ordenadores.

Y es que no es para menos, ya que este joven Hacker supuestamente coordino e inicio el mayor ataque a Internet que convulsiono al mundo de la informática, mas tarde al propio gobierno de los EE.UU., Bill Clinton y finalmente a los empresarios de la ReD que se hacían eco de las noticias de los ataques continuados.

Para llevar a cabo dichos ataques, MafiaBoy y Coolio «su aliado» utilizaron el método «denegacion de servicio» que consiste en bombardear los servidores atacados con peticiones falsas de información hasta colapsarlos, es decir, algo así como enviar un mailbombing. Con este sistema se paraliza su capacidad de respuesta, dejando colgado el servidor cuando se encuentra colapsado.

Atajar estos ataques informáticos se convirtió en la principal tarea de los expertos del FBI, que cuenta con 56 especialistas en combatir este tipo de delitos y que se vio obligado a emplearlos a todos ellos, para seguir la pista de MafiaBoy. MafiaBoy dejo pistas en algunos ordenadores de la Universidad de Santa Barbara y envío algunos E-Mails en la ReD mofándose de su hazaña, lo que hizo que finalmente los especialistas del FBI permitieran llegar hasta el cuarto de su casa, en el que MafiaBoy estaba constantemente conectado a Internet, evidentemente empleado métodos de Phreaking

5.9.4. Bill Gates, Steven Wozniak y Steven Jobs, los primeros Hackers adolescentes

El caso de Bill Gates es quizás una de las historias menos conocidas de este mecenas de la informática que ha sabido ligar el Hacktivismo, junto con sus compañeros de clase, a la historia misma de procesador y el nacimiento de Intel. Un poco enrevesada, la historia de Bill Gates bien merece la pena conocerla.

En 1956 se inventa el transistor y ocho años mas tarde aparecen los primeros circuitos integrados en el planeta. Al contrario que las válvulas de vacío, los nuevos dispositivos electrónicos, mucho mas reducidos y mucho mas rápidos, están basados en un material llamado silicio, y el silicio es extraído de la arena, pero Intel estuvo allí mucho después que la arena y algo antes que Steven Wozniak, Steven Jobs y Bill

Gates.

Pero la historia de Intel comienza en 1971 y su microprocesador 4004. Hace ahora 28 años, un ingeniero de la entonces sociedad estadounidense Intel «Integrated Electronics» Tedd Hoff, fue quien descubrió en 1971, tras mas de dos años de arduas investigaciones, el método de unir en una misma pastilla de silicio los diferentes elementos indispensables para crear lo que seria un «* microntrolador» un nuevo dispositivo que permitiría un tratamiento rápido de la información.

Hoff había concentrado sus esfuerzos en estudiar las memorias electrónicas destinadas a almacenar información y descubrió que si añadía una memoria electrónica junto a un procesador de calculo y unos cuantos enlaces, tendría sobre su mesa de trabajo un dispositivo realmente revolucionario después del circuito integrado.

Así nace el procesador 4004, compuesto por 2.300 transistores, todos ellos destinados a una unidad de calculo y una memoria electrónica. Este procesador estará destinado a equipar las primeras calculadoras. Este ingenio era capaz de procesar unas 60 000 operaciones por segundo, pero no eran suficientes operaciones como para crear un ordenador con el., de hecho aun no se había matizado esta idea hasta unos años mas tarde.

Un año mas tarde, en 1972 Intel saca adelante un nuevo modelo de procesador, esta vez llamado 8008. En aquel momento las industria informática, todavía no tenia en consideración el construir una computadora personal en torno a este u otro procesador. Pero de cualquier forma el 8008, la nueva creación de Intel aparecía en una popular revista de electrónica «Radio Electronics» como un avanzado procesador capaz de controlar cualquier sistema aritmético o de tomar decisiones inteligentes. Pero en cualquier caso ninguno de los lenguajes que en aquel momento existían, estaban preparados para dar ordenes a este procesador.

Bill Gates que por aquel entonces, junto a Paul Allen, eran unos jóvenes chavales enfundados en gruesas gafas de montura de hueso, ya trataban de hacer algo con el nuevo procesador de Intel, sin embargo los escasos transistores que albergaba en su interior no les permitieron crear un Software adecuado a fin de crear su mayor deseo, el de fabricar el primer ordenador personal basado en un Software que permitiera hacer llegar los ordenadores a cualquier usuario.

Pero no tuvieron que esperar mucho tiempo nuestros genios, hasta que Intel sacaba al mercado el que iniciaría una leyenda en esto de los microprocesadores, se trataba del 8080, un procesador con cerca de 10 000 transistores en su interior y toda una primavera de 1974 por delante.

El nuevo procesador de Intel había sido descubierto por Bill Gates a través de otra revista de electrónica, en esta ocasión la «Popular electronics» en la que se mostraba una especie de computadora con el nombre de Traf-of-data. Bill Gates quedaba

fascinado al ver el anuncio y advirtió que el final del reinado de las gigantescas computadoras estaba cerca.

El nuevo chip de Intel contenía 2.700 transistores mas que su antecesor y era unas 10 veces mas rápido que su homologo, lo que permitía acercarse un poco mas a la idea que Bill Gates tenia del futuro de las computadoras. Un año mas tarde, en 1975 aparecía otra nueva computadora en la portada de Popular electronics, en esta ocasión era la Altair 8800 y también Bill Gates se hacia eco de ello. Ese mismo año Bill Gates junto a Paul Allen escribía un nuevo Software para Altair. Un año mas tarde Steven Wozniak y Steven Jobs presentaban su Apple 1.

5.9.5. Entonces, un niño es un Hacker

Como habrá podido comprobar, algunos Hackers, además de comenzar su nueva faceta a una edad temprana han condicionado la evolución de la tecnología como Bill Gates y Steven Jobs, otros simplemente han demostrado que las nuevas tecnologías parecen estar hechas para la nueva generación.

Así, parece evidente, tras leer estas historias, que los grandes gurús de la informática y la tecnología de nuestros tiempos, son o han sido adolescentes con grandes facultades, Hackers de pronta edad que han marcado un hito a seguir. El Hacker mas joven es el ganador. Ya se declaró en su día que si ser curioso e interesarse por comprender comofunciona una cosa era ser Hacker, entonces un niño que pregunta a su padre el porque de las cosas, es un Hacker.

5.9.6. El final de las recopilaciones

Bueno, si ha llegado hasta aquí, espero que haya disfrutado con todas estas historias y que forman parte del mundo Underground desde ahora. Todas estas

historias, son casi un anexo al capitulo de historias de Hackers y Crackers. Por otro orden de cosas, aquí no encontrara todas las artimañas realizadas por los Hackers en los últimos años, y ni mucho menos la de los ultimo meses, a todo esto cuando cada día se suceden nuevas situaciones en la Red de Internet y fuera de ella. Recopilar aquí todo lo que ha sucedido y que sucede en la actualidad, seria simplemente, una tarea imposible, amen de las dos mil paginas que necesitaría para ello. No obstante, de a buen seguro que aquí tiene las historias más llamativas de la historia del Hacking.

Capítulo 6 Criptografía

Desde tiempos inmemorables siempre se busco, la forma de cifrar o «ocultar» un mensaje mediante técnicas reversibles, pero que a su vez volvían los textos ininteligibles. Cifrar un texto o mensaje, conlleva a que si este es interceptado por alguien, el texto no pueda ser descifrado sin la clave correcta.

Los sistemas criptográficos se han extendido como la pólvora en la Red, buenos y malos emplean la criptografía para «esconder» sus mensajes. Los Crackers más hábiles, por otro lado, tratan de demostrar que también los sistemas criptográficos mas modernos caen ante ellos.

Una buena muestra de ello es el Crack del código DES en 56 horas. De modo que la polémica esta servida. Pero por otro lado tenemos que, en su día se trataron sistemas de criptografía o cifrado, pero en señales de televisión, refiérase a Hackers, piratas tecnológicos. Donde se exponían los diferentes sistemas de cifrado reversibles.

Al igual que sucede con la televisión de pago, las comunicaciones, los programas y la propia Red de Internet, debe poseer una seguridad que proteja la intimidad de los datos. Los canales de televisión se pueden proteger mediante modificaciones en la señal compuesta. Estos procesos de encriptación de componentes son reversibles con el fin, naturalmente, de obtener la información en clara en el lado autorizado para tal fin.

Este mismo proceso debe seguir el campo de la informática, pero se detiene uno a pensar que aunque la palabra seguridad habita en todos los lugares, poco se parecen ambos métodos empleados, naturalmente por ser de diferentes naturalezas. Un canal de televisión esta compuesto por ciertas funciones analógicas y unos componentes indicativos de la señal. Todos estos componentes pueden ser sustituidos por otroselementos o transformados. A esto se le llama proceso de enmascaramiento o encriptación.

En la informática, aunque no existan los mismos elementos de una señal de video, también es posible encriptar la información. A este proceso se le denomina Criptologia. Criptologia es el arte de transformar un mensaje claro en otro sin sentido alguno. Este mensaje debe ser reversible en el otro extremo igual que si no hubiera sucedido nada. Es más fácil encriptar un texto que una señal de video, pero siempre resultara mas complicado desencriptar el texto que la señal de video. En una señal de video siempre puedes ver que sucede, pero en un texto normalmente no puedes adivinar nada, ademas los ficheros aparecerán encriptados y no podrán ser leídos por comandos estándares.

Pero la Criptologia o los programas criptográficos no son toda la seguridad que se pretende crear. Existen a su vez diversos complementos que aumentan la seguridad de

un terminal informático. Un ordenador es un equipo sofisticado que procesa datos, y como los descodificadores puede tener palabras de acceso que pueden bloquear el sistema si no se conocen. En los descodificadores esto, se llama, bloqueo paterno, mientras que en los ordenadores es una clave de acceso para empezar a trabajar con él. En ambos equipos se debe introducir una clave o contraseña antes de iniciar la sesión. en los descodificadores suelen ser claves de cuatro dígitos por la baja seguridad que necesitan. Normalmente estas claves son para evitar que alguien ajeno a la familia manipule el descodificador o receptor. Pero en los ordenadores, como se guardan valiosos datos, la seguridad debe de ser mayor.

En estas circunstancias debemos saber que un terminal de ordenador posee dos puertas de acceso al corazón del sistema. Uno, es a través del teclado, que es la puerta de introducción de datos más usual y la otra puerta, es el Moden que comunica al ordenador con el mundo exterior gracias a Internet.

En el primer caso, se debe introducir una contraseña de mas de cuatro dígitos si se desea, para poder acceder al sistema operativo. Esta protección es valida, para que nadie pueda entrar en nuestro ordenador desde el teclado sin nuestra autorización. Este método es ciertamente seguro para nuestra intención.

Pero en la Red existen peligrosos Hackers capaces de hacer cosas impensables, por ello la puerta segunda, requiere un mayor grado de seguridad. Normalmente, en base el buen entendimiento entre dos ordenadores, dos terminales deben poseer un inicio y salutación para que dos terminales se identifiquen y puedan trabajar conjuntamente. Esalgo así como un teléfono, si este no marca un número definido por el usuario, jamás nos pondríamos en contacto con la persona deseada.

En los ordenadores ocurre exactamente lo mismo. Cada ordenador debe tener asignado un nombre de identificación y ademas debe ser capaz de dialogar con el otro terminal, en los extremos mas simples como enviar un saludo, acuse de recepción y otros detalles. Sin estos detalles un terminal no podría identificar nunca al del otro extremo, ni dejar constancia de ello. De esta manera se controla el trafico y se evitan nudos indeseables en las comunicaciones. Pero esta puerta hasta ahora no poseía mas seguridad que los números de identificación del terminal a la dirección que le corresponde.

Y estos números son fácilmente reconocibles como se conoce el numero de teléfono de cada persona gracias a la guía telefónica. Los Firewalls o muros de fuego, son la solución para tapar el agujero de esta segunda puerta. Este programa puede identificar quien solicita el servicio de nuestro ordenador ademas e impedir que entren datos a nuestro ordenador. Por otra parte estos firewalls pueden reconocer comandos dañinos o peligrosos para nuestro terminal. Sin embargo, eso no termina de cuestionar la seguridad total.

Podemos impedir que un intruso entre en nuestro sistema, pero, ¿ que sucede

cuando tenemos que enviar algo a otro punto de la red?. Inevitablemente nuestro trabajo corre peligro de ser capturado por alguien externo a nuestro deseo. El programa PGP de Zinmerman es una solución muy buena a nuestro problema. Nuestro terminal ademas de velar por la seguridad de las dos puertas hacia el exterior, debe ser capaz de generar archivos ininteligibles por cualquier otro ordenador remoto que no tenga la autorización correspondiente.

Estos programas criptográficos son capaces de encriptar textos u otra información, gracias al empleo de algoritmos de encriptación altamente seguros. Podemos encontrar varios sistemas empleados y los vamos a tratar a continuación.

6.1 Un poco de historia

Ya en el antiguo Egipto se emplearon sistemas criptográficos y prueba de ello son los jeroglíficos no estándar escritos en las paredes de las pirámides y algunas tumbas. Esto, data de 4.000 años atrás y el sistema se basaba en figura geométricas y dibujos, queconformaban un mensaje no descifrable. Este sistema, podría ser realmente complejo ya que una forma geométrica indefinida podría decir muchas cosas y no decir nada.

Por otro lado los griegos ya empleaban sistemas criptográficos, aproximadamente en el año 500 a.C. Estos empleaban un curioso artilugio llamado «scytale» que consistía en un cilindro alrededor del cual, se enrollaba una tira de cuero. Se escribía un mensaje sobre la tira, y al desenrollarla, se podía ver una ristra de letras, aparentemente sin sentido alguno. Nótese que ya desde esa temprana edad, los sistemas de cifrado se sostenían sobre la base de intercambiar las palabras de los textos, y por tanto se trataban de sistemas de cifrado clásicos, ya que únicamente se necesitaban encriptar mensajes escritos.

Julio Cesar también empleo un sistema de cifrado durante su reinado. Dicho sistema ya ha sido convenientemente detallado en párrafos anteriores, dentro de uno de los métodos clásicos. Pero vamos a recordarlo aquí y ahora. Su sistema se basaba en sustituir la letra a encriptar por otra letra distanciada a 3 posiciones mas adelante. De esta forma se obtenían mensajes ininteligibles y durante su reinado y posterior el sistema nunca fue desencriptado por aquel entonces.

En el siglo XII, el sabio ingles Roger Bacon, describió diversos métodos

criptográficos al igual que Gabriel di Lavinde «quien inventó el sistema Nomemclator», quien publicó en 1379 una compilación de sistemas a petición del Papa Clemente VII. Es bien curioso saber que hasta la propia iglesia tenía que echar mano a sistemas criptográficos. Los sistemas empleados por esas fechas indudablemente se basaban en métodos clásicos por sustitución.

En 1467 León Battista Alberti invento el primer sistema criptográfico polialfabetico y no fue hasta el siglo XVIII, cuando fue descifrado. En 1790 Thomas Jefferson invento su cilindro de transposiciones, que fue ampliamente utilizado durante la segunda guerra mundial por la armada de los Estados Unidos. Pero el sistema no duraría mucho, ya que se basaba en un sistema polialfabetico y en 1861 se publicó la primera solución generalizada para resolver cifrados polialfabeticos, poniendo fin a 400 años de silencio. Sin embargo los sistemas criptográficos no experimentaron ni parada alguna ni mucho menos demora en sus sistemas de cifrado. Las grandes guerras impulsaron la creación de nuevos sistemas criptográficos más potentes y difíciles de entender. La maquina Enigma desarrollada por los alemanes a mediados de los 70 fue un duro golpe para el criptoanálisis y sobre todo para los expertos en sistemas criptográficos.

Poco después de los 70 aparecieron los sistemas criptográficos denominados modernos. Así en 1976 el código DES hizo su aparición gracias al desarrollo de computadores digitales. A partir de hay los algoritmos y sistemas de criptografía experimentarían un interés ineludible. El sistema DES fue el primero de los sistemas complejos, pero introdujo la clave secreta, que debía, esta, ser muy guardada si se quería mantener la fuerza del sistema, pero ese mismo año hacían la aparición estelar Diffie y Hellman, creadores del primer sistema de cifrado basado en claves publicas. Sistemas altamente seguros.

Un año después Rivert, Shamir y Adelman se sacaban de la manga el sistema criptográfico de actualidad, el RSA. Un sistema basado en buscar números primos, nada fácil de solucionar. Hasta la fecha el sistema esta siendo empleado por computadores y sistemas de codificación de canales de televisión.

Finalmente, el sistema criptográfico más conocido en la red de Internet para todos los cibernautas, es el sistema PGP de Phil Zimmerman, creado en 1991. Sin embargo hay que decir que este sistema criptográfico, mas que eso, es un programa que reúne los sistemas criptográficos más fuertes del mercado como el DSS o el de Diffie-Hellman. Pero lo que hace es jugar con ellos y así se obtienen brillantes encriptaciones realmente seguras.

Hoy por hoy el sistema objetivo por un gran numero de Hackers es el mencionado PGP, ya que es el mas ampliamente utilizado por los navegantes. De momento no se ha conocido apertura ninguna de este sistema, sin embargo los nuevos ordenadores del futuro, ponen en manos de Hackers herramientas verdaderamente potentes que

acabaran con todos estos sistemas criptográficos de gran seguridad.

Si no, tiempo al tiempo.

6.2. Criptografía, sistemas de cifrado

Criptografía significa literalmente «escritura secreta», es la ciencia que consiste en transformar un mensaje inteligible «en otro que no lo sea en absoluto», para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

Esta es la definición más correcta de la criptografía, ya hemos comentado porque debemos echar mano de ella, y ahora vamos a explicar que sistemas existen y de que forma se efectúan los mensajes criptográficos. Los Hackers los muy habilidosos para descifrar estos textos, pero lo cierto es que hace falta poseer un buen programa para poder descifrar incluso mensajes cifrados de forma sencilla.

Existen dos tipos de criptosistemas, simétricos y asimétricos. Los sistemas simétricos, son sistemas de cifrado basados en «claves secretas», estos, emplean la misma clave para encriptar y desencriptar el mensaje o los datos de control del descodificador. Los sistemas asimétricos, sin embargo, operan con dos claves distintas. Emplean una «clave pública» para encriptar y otra «clave secreta» para desencriptar. Este cifrado es mas complejo y por tanto posee un mayor nivel de seguridad.

Los sistemas de cifrado simétricos, como se habrá intuido son más débiles que los sistemas de cifrado asimétricos, esto es así, porque ambos, emisor y receptor deben de emplear la misma clave, tanto para el proceso de encriptación como para el proceso de desencriptación. De esta forma esta clave debe ser enviada a través de un medio de transmisión. Un Hacker podría leer esta clave y emplearla para desencriptar el mensaje. Si ciframos esta clave con otra clave, siempre estaríamos igual, ya que la ultima clave revelaría siempre la clave oculta. Sin embargo los sistemas de cifrado asimétricos, al emplear distintas claves, permite el uso de medios de transmisión poco seguros.

Después de estos sistemas de cifrado enunciados, podemos encontrar otros no menos importantes, que siempre se han empleado para cifrar textos o mensajes. Estos sistemas de cifrado son útiles para ordenadores y equipos de impresión de textos.

Los sistemas de cifrado simétrico y asímétricos son sistemas útiles para encriptar datos e información digital que será enviado despufés por medios de transmisión libres. Pero el texto siempre se cifro de alguna manera, y aquí también surgen grupos de interés. Podríamos hacer una división en dos grandes familias. En primer lugar tenemos los «métodos clásicos» y en segundo lugar «los métodos modernos». Es obvio que sabemos a que nos referimos. Los métodos clásicos son aquellos que existieron desde siempre y son métodos desarrollados para cifrar mensajes escritos a mano o en maquinas de impresión. Los métodos modernos son los ya mencionados sistemas simétricos o asímétricos.

Los métodos clásicos se basan en la sustitución de letras por otra y en la transposición, que juegan con la alteración del orden lógico de los caracteres del mensaje. Así a los métodos clásicos les han salidos dos formas de cifrado, denominados grupos, que son «métodos por sustitución» y «métodos por transposición».

Los métodos por sustitución son aquellos que cambian palabras por otras, esta simple forma de cifrar siempre ha obtenido buenos resultados. Los métodos por transposición son aquellos que alteran el orden de las palabras del mismo mensaje.

Los métodos modernos se basan en combinar secuencias de dígitos creados de forma aleatoria con los dígitos del mensaje, mediante puertas lógicas, en el caso de los módulos PRG sencillos. Otros emplean algoritmos matemáticos de gran complejidad para permutar mensajes de cierta longitud de bits.

Dentro de los métodos clásicos podemos encontrarnos con varios sistemas como los que siguen a continuación;

Cifrado Cesar o monoalfabetico Simple.
Cifrado monoalfabetico General.
Cifrado por sustitución polialfabetica.
Cifrado inverso.
Cifrado en figura Geométrica.
Cifrado por filas.

De los seis sistemas de cifrado mencionados los tres primeros están basados en los métodos por sustitución y los restantes están, obviamente basados en los métodos de transposición. Explicaremos cada uno de ellos y veremos que efecto de cifrado se obtienen en los mensajes.

El sistema de cifrado Cesar o monoalfabetico simple: es un método extremadamente simple y fue empleado por los romanos para encriptar sus mensajes, de hay el nombre de Cesar, ya que fue en su reinado cuando nació este sistema de cifrado. Este sistema de cifrado se consiste en reemplazar cada letra de un texto por otra que se encuentre a una distancia determinada. Se sabe que Cesar empleaba una

distancia de 3, así;

Sustituir A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z

Por

D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z C B A

Así el mensaje El Hacker acecha de nuevo, quedaría de la siguiente manera;

HÑ KDFNHU DFHFKD GH PXHYR

El sistema de cifrado monoalfabetico general; es un sistema que se basa en sustituir cada letra por otra de forma aleatoria. Esto supone un grado mas de complejidad en el método de cifrado anterior. Un ejemplo seria la siguiente;

Sustituir A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Por

Z C Q V A J G Ñ W N FB U M R H Y O D Y X T P E S L K
Y empleando el mismo mensaje anterior quedaría de la siguiente forma;

AF ÑZQNAO ZQAQÑZ VA UXATR

El sistema por sustitución Polialfabetica; es un método que emplea mas de un alfabeto de sustitución. Esto es, se emplean varias cadenas de palabras aleatorias y diferentes entre si, para después elegir una palabra distinta según una secuencia establecida. Aquí nacen las claves secretas basadas en números. Este sistema es algo mas complejo que las anteriores y a veces resulta difícil descifrar mensajes cuando empleamos mas de diez columnas de palabras aleatorias. Un ejemplo de ello es lo que sigue;

Sustituir A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z

Por

1/ F Q R A L K Z S J Ñ M Y T Y V D B E W V N O C X H P G
2/ G A W H V M U Y F Q L B R C J N D S K T Ñ P Z O Y X E
3/ C Ñ O G D Q H A R P Y T X E W V B M V L Y F S N Z K J

Con una clave 2-3-1, el mensaje seria así;

HY SGOMHM FWDRVAF HD YPDCJ

El sistema de cifrado inverso; es quizás una de las formas mas simples de cifrar una imagen y es probablemente reconocida por todos nosotros. Es normal escribir del revés cuando estamos aburridos, pero lo cierto es que este es un sistema de cifrado. La forma de hacerlo es simplemente escribiendo el mensaje al revés.

El hacker esta al acecho (oveun de ehceca rekcah le)

El sistema en figura geometrica; ya es mas complejo que la versión anterior. En esta ocasión el mensaje ya se empieza por escribir siguiendo un patrón preestablecido y sé encripta siguiendo una estructura geométrica basado en otro patrón. Este último patrón puede ser verdaderamente complejo según la extensión del mensaje escrito y la forma de seguimiento de la línea. Un ejemplo simple seria el que sigue;

El HACKER ESTA AL ACECHO

Patrón de cifrado;

Mensaje cifrado;

ECALHKAHOACRECEATSE

El método por transposición de fila; consiste en escribir el mensaje en columnas y luego utilizar una regla para reordenarlas. Esta regla elegida al azar será la clave para cifrar el mensaje. También aquí es importante saber la clave secreta para poder descifrar el mensaje. En esta ocasión el mensaje puede estar fuertemente encriptado si se emplean textos relativamente largos. Un buen ejemplo sencillo es el que sigue;

ELHACK Si la clave es 6 3 1 5 4 2

KHECAL

ERESTA AEETSR

ALACEC CAAECL

CHO OCH

Como hemos podido ver, todos los métodos criptográficos clásicos emplean la misma clave para cifrar y descifrar un mismo mensaje. Con la llegada de los

ordenadores, la resolución de estos sistemas se torno prácticamente trivial y por eso han surgido nuevos métodos de encriptación mas trabajados y seguros. Algunos de ello también basados en claves secretas, cuya computación es prácticamente inalcanzable o bastante compleja.

Tal como se ha dicho los métodos modernos son más complejos de elaborar y un buen ejemplo de ello se puede ver en el capitulo 11 de este libro, ademas de los ordenadores las tarjetas de acceso electrónicas, son capaces de trabajar con estas encriptaciones por la elevada velocidad de computación que presentan. Al estar basados en complejas transformaciones matemáticas de una secuencia, es indispensable disponer de memoria volátil y capacidad de procesamiento. Estos sistemas de cifrado modernos, son capaces de cifrar palabras de mas de 128 bits y normalmente se cifran en bloques.

Aunque aquí no vamos a detallar de nuevo estos sistemas criptográficos si vamos a enumerarlos, por supuesto los más importantes, empleados en la red de Internet. Para ello vamos a dividir la situación en tres grupos, uno que nombrara los sistemas de cifrado basados en claves publicas, otro grupo de cifradores basados en claves secretas y un último grupo mas reciente y empleado en la televisión digital, los métodos empleados en algoritmos. Sistemas de cifrado de clave pública;

* **RSA**: es quizas el sistema de cifrado mas empleado en la actualidad. Este sistema es el elegido para trabajar con los códigos del sistema de codificación Videocrypt, algoritmo que el Capitán Zap consiguió romper. Aunque después de ello se dice que sigue siendo el sistema de cifrado mas fuerte del mundo, existe una anécdota que hace pensar lo contrario. En 1997 un chaval de 16 años, un cerebro de la informática, fue capaz de romper el código RSA con una longitud de 200 bits en menos de cuatro horas.

El sistemas RSA se basa en la multiplicación de números primos, por lo que conlleva grandes operaciones matemáticas. Fue inventado en 1977 por Rivest, Shamir y Adelman, de hay el nombre RSA. También es cierto que el sistema de cifrado comentado ha sido modificado por sus inventores aumentando el grado de seguridad. El sistema permite utilizar documentos de diferentes tamaños; 512 bits, 768 bits, 1029 bits, 2048 bits…

* **Diffie-Hellman**: Data de 1976 y se emplea fundamentalmente para el intercambio de claves. Como ya se ha comentado y se comentara en otras paginas, es bastante delicado enviar la clave que permite el descifrado de un mensaje. Por ello se creo este sistema de cifrado empleado únicamente para proteger claves. Otros métodos no menos importantes son los siguientes;

* **Sistema de curvas elípticas**: está diseñado exclusivamente para cifrar textos escritos en ordenador y no se emplea para sistemas de encriptación de señales de televisión analógicas o digitales. El sistema se basa en los movimientos del ratón que

el usuario hace antes de la instalación del programa. Este sistema puede resultar realmente complejo.

*** DDS**: el sistema no ha sido publicado hasta ahora, pero se sabe que se basa en transmutar la secuencia de los dígitos o bits. También emplea métodos de permutación y rotación de dígitos en un módulo pseudoaleatorio. Ya hay Hackers que han trajinado con el…

*** El gamal**; parece un sistema español por lo menos por el nombre, pero no es así. También se basa en palabras de longitudes mas o menos extensas para el cifrado de mensajes. También esta desarrollado para sistemas informáticos y transacciones.

*** LUC**: solo se sabe de el que fue creado en 1993. Los sistemas de cifrado basados en claves secretas también han conocido una muy buena aceptación, gracias a la tecnología de los ordenadores que permiten hacer computaciones elevadas sea cual sea la longitud de bits elegidas. Vamos a mencionar solo tres de ellos. El mas importante quizás sea el código DES. Este sistema de encriptación es habitual verlo emplear en sistemas de encriptación de señales de televisión para proteger los datos ECM de control de descodificación de la señal. Sin embargo según los Hackers todos los sistemas de seguridad tienen sus fallos y por lo tanto pueden dejar de ser seguros, si el pirata es lo suficientemente hábil.

*** DES**: este si que es un sistema de cifrado, altamente seguro, rey de los sistemas basados en claves secretas, que ha demostrado su fuerza en los últimos 20 años desde su creación. Hasta ahora no ha podido ser abierto. Básicamente es empleado para las transiciones de datos interbancarios y transferencias de alto riesgo. Las tarjetas de acceso inteligente de los telebancos también operan según esta clave, con una palabra de unos 200 bits. El sistema de encriptación de señales de video Nagravision lo emplea para proteger los datos ECM y EMM del sistema. El sistema de cifrado DES se basa en la permutación de la longitud de bits, unos 200 por lo general, en al menos 16 permutaciones en la primera versión de este sistema de cifrado, después los datos son rotados a situaciones irrelevantes. El sistema esta descrito en el capitulo Carding, pero es mas que probable que a estas alturas hayan modificado la estructura del algoritmo de cifrado, pero de cualquier manera es prácticamente imposible de abrir aun cuando se sabe que ruta siguen los bits, en toda la secuencia.

*** IDEA**: este sistema fue desarrollado en Zurich en 1990 y emplea claves de encriptacion de 128 bits de longitud y se considera muy seguro. Es uno de losalgoritmos más conocidos actualmente. El método de cifrado se puede esperar, esta basado en modificar la orientación de cada bit, y combinarla con una puerta lógica variable.

*** RC4**: este algoritmo fue desarrollado por el grupo RSA y un buen día fue publicado, por lo que su seguridad descendió vertiginosamente. El sistemas se basa en combinar cada bit con otro bit de otra secuencia. Acepta claves de cualquier

longitud y emplea un generador de números aleatorios. Es muy difícil de romper y su fuerte, esta en la velocidad de computación admisible. Ademas es el método empleado por el SSL de Nestcape en su versión con clave de 40 bits.

Ademas de estos sistemas de cifrado basados en claves publicas o secretas, existen otros sistemas de cifrado basados en algoritmos. Estos nuevos sistemas no emplean claves de ningún tipo, si no que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud arbitraria. Esto es, cada cierta cantidad de texto elegido de forma arbitraria, se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra longitud clave, esta palabra longitud tiene una extensión de x bits preestablecidos, de esta forma el texto es irreconocible ya que solo se pueden leer números secuenciales y no guardan relación alguna entre si. Este es el método, quizás, más complejo que existe hasta el momento. Trabajar con estos algoritmos requiere sistemas informáticos, esto es, ordenadores o tarjetas de acceso inteligentes que solo comuniquen el tipo de algoritmo empleado. Estos algoritmos normalmente se basan en complejas operaciones matemáticas de difícil resolución. Y el secreto precisamente esta hay, en que operaciones matemáticas sigue el algoritmo.

Entre los sistemas desarrollados a partir de la creación de algoritmos, cabe destacar al menos dos, por su complejidad e importancia sociales;

*** MD5**: este algoritmo esta desarrollado por el grupo RSA y es un intento de probar con otros sistemas criptográficos que no empleen claves. El algoritmo desarrollado es capaz de obtener 128 bits a partir de un determinado texto. Como es lógico hasta el momento no se sabe cuales son las operaciones matemáticas a seguir, pero hay alguien que dice que es mas que probable que se basen en factores de números primos.

*** SHA**: es un algoritmo desarrollado por el gobierno de los EE.UU y se pretende implantar en los sistemas informáticos de alta seguridad del estado como estándar de protección de documentos. El algoritmo obtiene 160 bits de un texto determinado. Se sabe que existen Hackers que han probado suerte, pero hasta el momento nadie ha dicho nada mas al respecto.

6.3. Criptoanálisis

Este si que es un tema complejo. Esta ciencia o parte de ella también denominada Hacking por los underground o Chiberpunks, es el arte de estudiar los mensajes ilegibles, esto es, encriptados, para transformarlos en legibles sin conocer la clave o el método empleado. Esto es, romper el cifrado y hacer Crack.

Como ya se ha comentado en otros capítulos de este libro, un buen principio es tener mucha paciencia y gran capacidad de intuición. Este último es quizás el factor más importante de todos, sin ella probablemente estés perdido. También es lógico que debes ser un experto en sistemas criptográficos, lo primero que puedes hacer es estudiar los sistemas ya existentes. Que probablemente te sirvan de algo.

Estudiar los sistemas de cifrado basados en métodos clásicos, te aportara una gran creatividad y es probable que puedas abrir cualquier mensaje encriptado en alguno de ellos. Sin embargo los textos encriptados con cualquier sistema basado en métodos modernos, ya es algo mas complejo. En tal caso debes emplear un ordenador como mínimo y crear un programa que resuelva con elegancia algunas combinaciones lógicas y algunas operaciones matemáticas.

La operación para abrir un sistema criptográfico te puede llevar días, cuando no semanas, ademas estos métodos modernos, sobre todo los métodos basados en algoritmos son muy difíciles de descubrir. Por otro lado, como ya se ha dicho, los métodos basados en claves publicas son los sistemas mas fuertes.

Los principales Hacks realizados en la red se basan en falsear lo IP, protocolos de entrada en ordenadores remotos. Muy pocos Hackers son capaces de descubrir y reventar los algoritmos o mensajes cifrados. Estos, son de reducido numero de componentes y normalmente no lo hacen para hacer daño, si no para demostrar que todos los programas tienen bugs. El hacker mas peligroso es el que crea virus informáticos y abre puertas lógicas y te modifica los ficheros de tu ordenador.

Los virus informáticos también pueden ser algoritmos complejos de desencriptar. Esto se crea así, para que los Sysops o policías cibernéticos no puedan descubrir la forma de anular o reconocer el virus. En este caso también se procede al criptoanálisis del virus.

Por otro lado los Hackers mas deseados siempre estarán bien protegidos, ya que son los mas adecuados para suministrar ayuda en operaciones delicadas como el espionaje del enemigo. Sin ir mas lejos en la guerra del golfo pérsico, fueron necesarios desencriptar muchos mensajes para frenar las fuerzas de Sadam hussein, algo que muchos han ignorado desde siempre.

Cualquier guerra mas o menos importante de hoy día y desde las míticas y no olvidadas guerras mundiales primera y segunda, siempre se han empleado encriptaciones en los mensajes. Y desde siempre existió el criptoanálisis para desencriptar los mensajes del enemigo. Una famosa alusión de ello, es el «Enigma» una maquina de escribir que imprimía la Z en lugar de la A, por citar un ejemplo.

Este hecho ha pasado a la historia de la criptografía y el criptoanálisis, por la dureza del sistema enigma, ya que el caso no es de menospreciar. En los años 20, los alemanes desarrollaron para aquella época, «la segunda guerra mundial» una maquina altamente sofisticada a la que llamaron «Enigma». Su misión, era la de crear textos cifrados de alta seguridad totalmente incomprensibles. Su aspecto exterior era la de una maquina de escribir convencioal, pero con la salvedad de que, al teclear la letra Z esta, imprimía una A y así con todas las letras del alfabeto. En un principio esto, podía tratarse de un método clásico siguiendo un patrón fijo, sin embargo el truco no estaba hay. La relación pulsación/resultado cambiaba de forma aleatoria y de eso se trataba. Con lo cual era prácticamente imposible descubrir un orden.

De esta forma Enigma fue el instrumento para cifrar las ordenes y mensajes durante la segunda guerra mundial y fue entonces cuando entro de lleno la ciencia del criptoanálisis y de los Hackers «oficiales».

Sin embargo fue en 1933 cuando un experto en criptografía, Marian Rajewsky, perteneciente al servicio de inteligencia polaco, consiguió descifrar los mensajes de Enigma. Para ello tardaron varios años de criptoanálisis continuados con el fin de clonar o fabricar una maquina exacta a la Enigma de los alemanes.

Pero la maquina experimento ciertas evoluciones y Marian Rajewsky junto con la ciencia polaca no pudo enterarse de la inminente invasión Nazi. Sin embargo los ingleses, muy activos a la hora de hacer hacking, siempre han sido los pioneros en sistemas de desencriptación de canales de pago, continuaron con la investigación del sistema Enigma mejorado, y por fin, en 1940, apareció el primer mensaje descifrado de las nuevas Enigma. Fue un genio llamado Alan Turing y un grupo de personas sacados de «debajo de las piedras» y que otra cosa podían ser que verdaderos Hackers.

También la Biblia pudo ser cifrada mientras se escribió, o esto es lo que afirma un tal Michael Drosnin, el cual asegura también, que ha conseguido mediante el criptoanálisis y la ayuda de una potente computadora, descifrar mensajes muy importantes para la humanidad, entre ellas cuando será el fin del mundo.

Capítulo 7 Bibliografía del Hacker

Siempre, o al menos casi siempre, un libro de esta envergadura y tema, esta escrito a partir de algunas referencias encontradas en otros libros, o dicho de otra manera, el proceso de documentación pasa por leer y releer cientos de paginas, ya sean de libros, recortes de periódico o contenidos de Internet. Esta es la base de todo historiador, periodista o investigador, y en este caso, no se iba a ser menos. Ademas, creo conveniente hacer desfilar a lo largo de unas cuantas páginas, los títulos de aquellos libros que pueden ser de interés especial, para la mayoría de los lectores de estos temas. Son libros que podrá adquirir en la librería de la esquina o en el peor de los casos, podrá adquirirlo en Amazon, la librería de Internet como así se la puede llamar. Durante unos meses escribí una serie de reportajes para la revista *Iworld*, y durante ese tiempo conocí a dos editores muy importantes con los cuales he trabajado muy a gusto, pero uno de ellos estaba realmente obsesionado con el tema Underground hasta tal punto de tener, literalmente, una librería en su casa formada solo por este tipo de libros. Libros sobre Hackers. En cierta manera conocí cuáles eran los títulos preferidos por este editor y en cierta manera los reflejo aquí, ya que después de ojearlos, en verdad, este editor tenia muy buen gusto y acierto a la hora de elegir un titulo entre diez. Ademas, me he tomado la libertad de añadir otros títulos que se publicaron después, los publique yo o los rescate de alguna estantería de una gran superficie. En definitiva son libros interesantes, los cuales me han reportado ideas, contenidos y en cualquier caso, buenos momentos de lectura.

7.1. Los nuevos manuales

Uno de los mejores libros podría ser Approaching Zero de Bryan Clough y Paul Mungo. Dos expertos escritores sobre temas de Hackers. En España este libro ha sido editado por la editorial Ediciones B, bajo el titulo Los piratas del CHIP. Es un libro muy recomendable y practico.

Approaching Zero Bryan Clough, Paul Mungo 1992. ISBN: 0571168132 1992. ISBN: 8440631529 España 242 páginas

Es tal vez el mejor relato sobre los phreakers (Hackers telefónicos), y uno de los

pocos libros que ofrece versiones completas sobre casos como el del robo del QuickDraw de Apple por parte de los Crackers, los primeros virus informáticas con nombres propios y la historia del Chaos Computer Club. El título hace referencia al posible borrado global de toda la información de los ordenadores del planeta por culpa de los ataques de los piratas, una de las catastróficas perspectivas que plantea el libro.

Secrets of a Super Hacker The nightmare 1994. ISBN:1559501065 204 páginas

Este libro es, sencillamente, un manual de Hackers. Escrito por un anónimo experto, explica todos los métodos clásicos de los Hackers, con un texto muy sencillo y fácil de comprender (incluso infantil, en algunos momentos). Entre las técnicas que se explican están los ataques por fuerza bruta a archivos de contraseñas, la ingeniería social, la interceptación de correo y contraseñas, el acceso a cuentas privilegiadas y otros cuantos trucos más. Incluye incluso una pequeña historia del Hacking y algunas técnicas básicas relacionadas con BBS, Unix y algunas listas de contraseñas comunes

The New Hacker's Dictionary Eric. S.Raymond 1994. ISBN: 0262680920 506 páginas

Esta segunda edición del Diccionario del Hacker es sin duda referencia obligada para todos los Hackers como para los quiero-y-no-puedo (una de las definiciones del diccionario). Es una edición de lujo del famoso archivo JARGON (jerga) de Internet, en el que durante décadas se ha ido incorporando información sobre la jerga de los Hackers, y usos y costumbres del lenguaje informática. Muchos de los términos y chistes proceden de las oscuras épocas de los orígenes de los Hackers, pero no dejan de tener su gracia. Incluye capítulos sobre costumbres gramaticales de los Hackers, el folklore relacionado, un retrato del prototipo del Hacker y bibliografía adicional. Al Macintosh se le califica en la jerga como Macintoy (considerado como juguete) o Macintrash (por los Hackers que realmente no aprecian separarse de los verdaderos ordenadores por una interfaz bonita). Un Hacker es, cómo no, una persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar toda su capacidad, frente a la mayoría de los usuarios que prefieren aprender sólo el mínimo necesario.

Hackers Steven Levy «La revolución de los héroes de las computadoras» 1994 ISBN: 0385312105 454 páginas

Si alguien captó y plasmó la realidad de los Hackers desde los años 50 (oh, sí, desde entonces) ese ha sido Steven Levy. Con un gran trabajo de investigación y una

atractiva narrativa, Levy recorre los primeros tiempos de los Hackers del MIT y el Tech Model Railroad Club (donde comenzó a usarse la palabra «Hackers») hasta terminar en la época gloriosa de los videojuegos para los ordenadores familiares. En el recorrido se diferencian en tres partes los «auténticos Hackers» del MIT, los Hackers del hardware, incluyendo a la gente del Homebew Computer Club (Wozniak, Steve Jobs, Bill Gates) y los Hackers de los videojuegos, centrándose en la gente de Sierra y la evolución de los juegos de ordenador. La «ética del Hacker», su forma de vida y su filosofía quedan plasmados en este libro mejor que en ninguno. Un documento histórico y absolutamente obligatorio

Underground Suelette Dreyfus 1997 ISBN. 1863305955 476 páginas

Esta novela, basada en hechos reales, cuenta las andanzas de un grupo de Hackers australianos y sus aventuras en las redes. Al igual que otras novelas sobre Hackers, Underground acerca al lector al «lado oscuro» de la Red describiendo varias historias de forma entretenida y explicando, de forma sencilla y elegante, los métodos utilizados y el entorno de cada aventura. Narra varios casos diferentes, situados en el tiempo a partir de 1989, sobre Hackers que se introdujeron en la red de la NASA (e introdujeron el «gusano WANK»), la conexión australiana con Hackers americanos, los BBS dedicados al lado oculto de la Red, utilizados por Hackers y Phreakers («piratas telefónicos») y muchas pequeñas historias de casos que tuvieron algo de publicidad en los medios de comunicación. Entre las más llamativas se encuentra el caso del «asalto» a la red de Citybank en Australia, donde los intrusos intentaron hacerse con más de medio millón de dólares. El libro no se dedica sólo a las aventuras divertidas: también indaga en las personalidades de los Hackers, su comportamiento habitualmente antisocial, sus problemas familiares y a veces con las drogas, así como la (inevitable) captura por parte de las autoridades, posterior juicio y estancia en prisión de la mayoría de ellos. La descripción de las detenciones, registros y procesos legales es especialmente interesante. El libro tiene como fuentes a varios grupos de Hackers australianos y todas las sentencias de los casos de asaltos informáticos de esa época.

The CucKoo-s Egg Clifford Stoll 1989 ISBN: 0671726889 394 páginas

Narrada en forma de novela, el «huevo del cuco» cuenta la historia de Clifford Stoll, un astrónomo e informático que, comprobando sus sistemas, descubre una diferencia de 75 centavos en la contabilidad. Este pequeño detalle le lleva a darse cuenta de que los ordenadores de su red están siendo atacados por Crackers del extranjero, y con ello comienza su particular carrera de persecución hasta dar con ellos. Escrito de forma entretenida y amena, describe la forma en que los Crackers se

introducen en los ordenadores y la forma en que pueden ser detectados. Interesante como documento histórico, es uno de los clásicos sobre el mundo del Hacking y el Cracking.

Cyberpunk Katie Hafner, Jhon Markoff1991 ISBN: 068418620 370 páginas

Los Cyberpunks son los forajidos y hackers de la frontera informática. Este clásico ensayo sobre phreakers (ackers telefónicos) y crackers (piratas informáticos destructivos) narra las aventuras de tres hackers bien diferentes: Kevin Mitnick, uno de los más conocidos hackers telefónicos; Pengo, el Hacker que flirteó con los espías de más allá del telón de acero y RTM (Robert T. Morris), quien creó el famoso gusano de Internet y puso de rodillas a toda la red mundial. Muy informativo y entretenido por su narrativa.

The Hacker Crackdown Bruce Sterling 1992 ISBN: 055356370X 316 páginas

Otro de los clásicos, se trata de un excelente acercamiento periodístico a la historia del Phreaking telefónico y el Hacking. Comenzando, literalmente, por la historia del teléfono, recorre los años 70, 80 y 90 contando las historias de los phreakers y hackers más conocidos (Fry Guy, Acid Phreak, Phiber Optik), las historias de los primeros BBS, las incursiones de los pioneros, las persecuciones policiales y del FBI y el famoso caso de los documentos E911 que dejó totalmente en ridículo a la justicia americana ante los hackers. Es un libro muy completo que describe la personalidad de muchos hackers, grupos y entidades del mundillo informático, como los círculos del boletín 2600, el WELL de San Francisco y la EFF (Electronic Frontier Foundation).

Masters of Deception michelle Slatalla, Joshua Quitter, Harper Collins 1995 ISBN: 0060926945 226 páginas

En este libro sobre los Crackers (piratas informáticos destructivos) y los phreakers (hackers telefónicos) se describen las andanzas por las redes de bandas como los MoD (Masters of Deception), la LoD (Legión of Doom) y las personalidades y técnicas empleadas por muchos de sus componentes, incluyendo algunos tan populares como Acid Phreak y Phiber Optik. Narra una auténtica batalla entre bandas rivales, lasreiteradas detenciones de muchos de sus miembros y la persecución por todo el ciberespacio por parte de los agentes del FBI, para terminar con la detención de los componentes de los grupos y su comparecencia ante la justicia.

Takedown Tsutomu Shimomura, John Markoff 1997 ISBN: 8403595980 versión español 464 páginas

El libro tiene un buen encabezado y dice así; Persecución y captura de Kevin Mitnick, el forajido informatico mas buscado de Norteamérica. Una crónica escrita por el hombre que lo capturo. Narrada con gran maestría, en este libro Tsutomu detalla, con la inestimable pluma de John Markoff, por supuesto, todo lo que sucedió en la noche de Navidad mas larga de su vida. Tsutomu estaba fuera de su casa, pero sus tres ordenadores estaban encendidos y alguien trabajaba con ellos…a distancia. Kevin Mitnick había conseguido penetrar en el sistema de Tsutomu, el hombre mas experto en seguridad informática, pero había algo en sus ordenadores que a Kevin le interesaba. Se trataba del Software de un teléfono móvil OKI. Y quizás esa obsesión por este Software marco el principio del fin del Hacker mas perseguido de toda Norteamérica.

En la actualidad, lejos de los teclados, Kevin cumple condena en la cárcel, pero esta siendo apoyado por docenas de WEBs que reivindican sus derechos y su libertad, hasta el punto que varios Hackers amenazan con colapsar la Red con «Gusanos» si no lo sueltan pronto. Por otro lado, como curiosidad cabe decir que Kevin tiene acceso al exterior a través de Internet, ¿ Como lo hará?. Un libro muy recomendable.

Enigma Robert Harris 1995 ISBN: 8401326672 español 388 páginas

Esta novela de intriga tiene como protagonistas a los expertos británicos que deben descifrar los códigos secretos de la máquina alemana Enigma mientras decenas de submarinos se dirigen hacia los convoyes aliados de las aguas del Atlántico Norte. Los personajes de la historia son ficticios, pero las máquinas, señales y mensajes alemanes son las originales de los textos históricos.

Codebreakers F. H. Hinsley. Alan Stripp 1993 ISBN: 019285304X 320 páginas

Este libro narra, en primera persona, la historia de Bletchley Park, el lugar en que se rompieron e interpretaron las transmisiones alemanas, italianas y japonesas durante la Segunda Guerra Mundial. Los protagonistas responsables de Ultra, el nombre en clave que los británicos dieron a todas las transmisiones de inteligencia de los enemigos del bando Aliado, cuentan cuál fue su importancia y cómo se descifraron sistemas criptográficos como los empleados en la máquina Enigma alemana y el tráfico Fish (no-morse). El libro es una recopilación de relatos de los trabajadores de Bletchley Park, algunos bien conocidos en el mundo de la criptología, otros, héroes anónimos. Bletchley Park llegó a romper la criptografía de 4.000 mensajes alemanes al día y desarrollar las «bombas» lógicas, Mark y Colossus, precursores de los

actuales ordenadores, con el único objetivo de romper códigos secretos. Como vino a decir Churchill, Bletchley Park y su gente fueron el arma secreta aliada que permitió ganar la guerra. En este libro queda narrada esta historia en primera persona.

The codebreakers David Khan 1996 ISBN: 0684831309 1184 páginas

The Codebrakers es un libro obligado de referencia histórica para cualquier interesado en la criptotología y sus orígenes. Cubre de forma extensa toda la historia de la criptología y sus protagonistas, desde el principio de los tiempos hasta la actualidad. La primera edición de The Codebreakers data de 1967, y la actual (1996) ha sido ligeramente revisada para incluir algo sobre informática, criptografía de clave pública e Internet. [En realidad no hay demasiados cambios sobre la edición original, unas 16 páginas nada más… digamos que se queda en 1967 aproximadamente. Sobre la criptografía moderna pueden encontrarse otros libros más completos]. Comenzando por los jeroglíficos del año 3.000 antes de Cristo, Kahn describe con una narrativa agradable y cuidada los pasos históricos por la criptografía, el criptoanálisis y todas las etapas de su utilización en tiempos de guerra y paz. La mayor parte del libro se centra en los siglos XIX y XX, y en la utilización de la criptología en las guerras mundiales. En su estudio de la criptografía el autor aprovecha para explicar todos los códigos y sistemas de cifrado clásicos, quiénes fueron sus inventores, cómo se descubrieron los sistemas de criptoanálisis y cómo se utilizaban. Todo ello, aderezado con breves biografías de los más importantes criptógrafos. La explicación de los métodos criptográficos está al alcance de cualquiera, y se incluyen abundantes ejemplos, referencias, imágenes y fotografías. Episodios clásicos como el Telegrama Zimmermann (probablemente el criptoanálisis más trascendente de la historia, en la I Guerra Mundial) o el funcionamiento y descifrado de las máquinas Enigma de los alemanes durante la II Guerra Mundial son tratados en profundidad y con todo lujo de explicaciones. El libro completa la visión histórica con explicaciones puntuales sobre la importancia de la criptografía en la sociedad, y está aderezado con varios apéndices sobre la anatomía y patología de la criptología, la criptografía aplicada a la comunicación con seres extraterrestres y una amplísima bibliografía.

Firewalls and Internet Security Willian R. Cheswick, Steven M.Bellovin 1994 ISBN: 0201633574 308 páginas

Describiendo como «cortafuegos» (firewall) un conjunto de componentes diversos, entre los que están los filtros y las pasarelas (gateways), este manual es más una recopilación de consejos prácticos sobre seguridad que una guía paso a paso sobre cortafuegos o productos concretos. Comienza explicando la necesidad de la

seguridad y la base de todo: el TCP/IP. La segunda parte explica la filosofía de los cortafuegos y las funciones de sus componentes, de forma más detallada, parándose en todos los servicios de Internet, indicando sus debilidades y dando ideas prácticas. La tercera parte es la más divulgativa, y describe lo que muchos administradores suelen pasar por alto: las más rebuscadas formas de robar contraseñas, la ingeniería social, los fallos y bugs de sistemas y protocolos, las puertas traseras y algunas formas concretas de ataque a servidores. La última parte está dedicada a las consideraciones legales (monitorización, pruebas) y, de forma destacada, a las comunicaciones seguras sobre redes inseguras. La introducción a la criptografía es muy interesante (y teórica), y se explican algunos sistemas como Kerberos (autenticación) y varios sistemas de cifrado a nivel de aplicaciones y transporte de red. Termina con una lista de software gratuito útil para los administradores de redes y seguridad, algunas recomendaciones generales (para fabricantes de sistemas) y una bibliografía extensa, donde se pueden encontrar muchos ejemplos teóricos y prácticos de ataques. Lo más interesante del libro: una serie de iconos de «alto peligro» (más de 40) que alertan en cada sección de los problemas más graves que suelen encontrarse en las redes.

PGP, Pretty Good Privacy Sims Garfinkel. O´Reilly 1995 ISBN: 1565920988 394 páginas

Este libro es un manual de referencia sobre PGP realmente completo y bien escrito, que cubre todas las variantes de la versión 2.6.2. Contiene todo lo que se puede necesitar saber sobre las primeras versiones de PGP y su utilización: todas las opciones, modos, uso de las claves públicas e instrucciones paso a paso para la generación de claves, gestión de los anillos de claves y uso de las firmas digitales. Además de esta parte práctica, el libro cuenta con varias secciones de interés general. En la primera, las bases de la criptografía, explica todos los términos y teoría de la criptografía clásica y moderna. Un par de capítulos están dedicados a la criptografía antes de PGP (historia y política) y otro al desarrollo de PGP en sí, incluyendos datos difíciles de encontrar en otros libros, como la historia detallada y pormenorizada de PGP desde las primeras ideas hasta la versión 1.0. Otro capítulo está dedicado a las implicaciones políticas de la «criptografía fuerte», y la inmiscusión de las «agencias de tres letras» en este terreno. Los apéndices del libro incluyen información detallada para instalar PGP (versión 2.6) en PC, Unix y un Macintosh.

Applied Cryptography Bruce Schneider. John wiley 1995 ISBN: 0471117099 784 páginas

Este es el libro de referencia obligatorio para cualquiera que quiera programar

algoritmos y protocolos criptográficos en su ordenador, o aprender cómo funcionan y cuáles son sus bases. Applied Cryptograpy está dividido en cuatro partes: Protocolos, técnicas, algoritmos y «el mundo real». La parte de protocolos explica los sistemasbásicos y avanzados de intercambio de claves, autentificación, firmas, etc. La parte de técnicas describe sistemas de gestión de claves, cifrados de bloques y de flujo, funciones hash y el uso del cifrado en sistemas convencionales. La tercera parte, más técnica, describe los algoritmos criptográficos, su base matemática y algunas implementaciones. Entre los algoritmos más destacados están el DES y sus variantes, Diffie-Hellman, RSA, RC2 y RC4, IDEA, Skipjack (Clipper) y funciones hash como MD2-MD5 y SHA. La parte del «mundo real» explica algunas implementaciones clásicas, como Kerberos, PEM, MSP, PGP, Clippper y Capstone. También hay algo sobre criptografía y política en uno de los capítulos finales, incluyendo referencias a páginas WEB, boletines, asociaciones y grupos de noticias de Usenet. La parte final del libro incluye listados del código fuente en C de muchos de los algoritmos explicados en la tercera parte del libro: Enigma, DES, NEWDES, IDA, MD5 y otros.

The Book of prime number records Paulo Ribenboim. Springer-Verlag 1988 ISBN: 0387965734 478 páginas

Este curioso libro presenta, como su título indica, los récords relativos a los números primos. Pero contiene mucho más: todas las preguntas frecuentes, respuestas y demostraciones de teoremas relativos a los números primos. Comenzando por «cuántos números primos hay» explica en lenguaje matemático (de alto nivel) un gran número de formas de comprobar si un número es primo (importante en criptografía), explica los diferentes tipos de primos y su distribución e incluye diversos apéndices con problemas, conclusiones y tablas.

Protect you Macintosh Bruce Schneier 1994 ISBN: 1566091012 316 páginas

Libro de referencia para los usuarios de Macintosh y responsables de sistemas interesados por los temas de seguridad. Describe técnicas de encriptación de archivos, protección ante virus informáticos, copias de seguridad, seguridad física y seguridad en red. Incluye muchos consejos y referencias a software y hardware comercial, con ejemplos, descripciones y precios.

Codes, Ciphers and secret writing Martin Gardner 1972 ISBN: 0486247619 98 páginas

Pequeño libro de Martin Gardner (autor durante muchos años de la columna «Recreaciones Matemáticas» de Investigación y ciencia) en el que en forma de

juegos explica los códigos y sistemas de cifrado más sencillos. Contiene muchas ilustraciones y problemas sencillos de resolver. Aunque antiguo, resulta entretenido y muy recomendable para principiantes. Es tal vez la forma más amena de comprender y jugar con los sistemas de cifrado clásicos. Podría considerarse un The Codebreakers simplificado, porque el recorrido que hace por la criptografía sigue también la línea histórica. Para los amantes de los secretos, también se incluyen un buen número de sistemas «alternativos» de envíos de mensajes, especialmente de steganografía.

Hackers Piratas Tecnológicos Claudio Hernández 1997 ISBN: 417 páginas

Un libro indispensable para los futuros Hardware Crackers y además uno de los muy pocos libros editados en Español sobre el tema de Hacking y el primero que revela aspectos técnicos de los Cracks. El libro repasa sobremanera a una buena cantidad de Hardware Crackers y sus logros. También se exponen circuitos y tácticas para descodificar casi todos los canales de televisión de pago. Se da un repaso a las tarjetas electrónicas de pago y se trata con delicadeza las técnicas de Hackeo.

Hacking en Internet Robles, Claudio Hernández 1998 ISBN: 417 páginas

Hacking en Internet es un libro genérico que pretende dar un enfoque divulgativo sobre los temas legales, ilegales y las tecnicas del Hacking. No es una Bíblia para aprender a Hackear. Sin embargo encontrara buena información en él. El libro ha sido escrito por varios autores, en lo que se deduce hay diversidad de información, y por supuesto,diferencia de estilos entre los tres autores que escribieron el libro. Por lo que a mi me toca contar, puedo decir, que escribí cerca de 100 páginas para este libro, y que en esas 100 paginas, trate de contar mucha cosas acerca de todo lo que rodea el Hacking e Internet como tal. Evidentemente reconocerá, «si ha leído Hacking en Internet» algunos principios inseparables de mi biografía, también aquí reflejados en esta obra que tiene entre sus manos. Esto no significa falta de recursos ni bloqueo de escritor, sino mas bien, que creo interesante recalcar ciertos aspectos en una obra de idéntica condiciones que la citada. Así pues, se recobran aquí los Virus informáticos, los clanes de la Red y otras cuestiones no menos importantes en un libro de esta envergadura.

Crack TV -Hackers Piratas Tecnológicos 2- Claudio Hernández 2000 ISBN: 417 páginas

Como su titulo indica, es la continuación de Hackers, Piratas tecnológicos. Digo continuación, porque en esta segunda edición, se han cambiado muchas cosas con respecto a la primera edición. En realidad se han añadido mas de 200 nuevas páginas, todas ellas centradas a destacar a los crackers y los propios cracks de las televisiones

de pago. En los últimos meses, se multiplica la creación de Foros que hablan sobre este tema. En el libro, se recogen pues, toda aquella información, que se encuentra esparcida en la ReD, que es Internet y que a menudo, uno, nunca sabe como llegar hasta ella. En definitiva, es un libro que le ahorrara horas de navegación, pero a su vez le mostrara los aspectos más oscuros del Cracking de los sistemas de encriptación de vídeo y audio, entiéndase televisiones de pago o plataformas digitales.

El libro recoge los mejores manuales de MaCDeC y OverrideSidek, dos nombres muy respetados en el entorno Underground «en lo que se refiere a la televisión encriptada» los cuales, coescribieron los primeros escritos sobre sistemas y Cracks para la televisión encriptada. Mas adelante se recoge información de varias páginas, que aseguran haber roto los sistemas de cifrado de las actuales plataformas digitales Españolas, entiéndase CSD «Canal Satélite Digital» y Vía Digital, así como otras plataformas Europeas como Irdeto, Conax o Cryptoworks.

El libro no le enseña como piratear estas señales, pero si le muestra el estado en como se encuentran, así como los Hacks y Cracks en torno a estos sistemas. Por otro orden de cosas, en el libro se hace un largo repaso, a otros Cracks no menos importantes como elDVD, las Videoconsolas o los CDs. En definitiva, Crack TV, es el punto de referencia para los fanáticos de los Cracks de moda.

A prueba de Hackers de Laras Klander 1998 ISBN: 38.081.1998 568 páginas

A prueba de Hackers, es el libro más vendido del año por varias razones obvias. Este libro contiene sutil información sobre Virus informáticos, defensa contra Hackers y tácticas de reconocimiento de intrusos. Es en definitiva, un gran libro, escrito con un lenguaje sencillo y en el que se exponen numerosos ejemplos prácticos. Con la lectura de este libro, conocerá que es un Virus, un gusano o un caballo de Troya. También conocerá las técnicas de los Hackers para atacar maquinas remotas, y al mismo tiempo aprenderá a defenderse de estos ataques. Klander hace especial hincapié en el uso de Software de protección, denominados Firewalls, Klander les dedica buena parte del libro. También se tienen en cuenta la seguridad SSL en Internet, las firmas digitales, los Scripts de Java o los protocolos HTTP y sus vulnerabilidades. A prueba de Hackers, es en definitiva, la unificación de varios libros de Hacking en uno solo.

Hackers de Stuart McClure, Joel Scambray y George Kurtz 2000 ISBN: 84-481-2786-2 514 páginas

La tendencia a que importantes Hackers se reciclen de alguna manera y pasen a formar parte del gremio de escritores, es apabullante. Estos tres hombres, todos ellos ex- Hackers como se les podría denominar, han pertenecido al sector de la élite y

ahora aportan sus conocimientos en una obra llamada, Hackers. En el libro exponen las mas variadas técnicas para atacar y defenderse de ataques. Con el subtitulo de Secretos y soluciones para la seguridad de redes, nuestros hombres formulan toda clase de propuestas a los administradores de redes. El libro puede ser empleado con ambos fines, es decir, para aprender técnicas del Hacking y para prevenirlas. De cualquier forma se especula sobre su mal uso y se advierte al lector, y al que no lo es, de que su fin es deinformar al administrador de redes. En cualquier caso, se revelan las mejores tecnicas del Hacking entre ordenadores.

Secret and Lies de Bruce Schneier 1997 ISBN: 417 páginas

Entre la reflexión y la criptografía, Bruce Schneier nos asombra de nuevo. En su libro Secretos y mentiras, repasa la criptografía, la seguridad y los posibles puntos fuertes y débiles que parecen surcar por el cibernegocio. Es en definitiva, una reflexión de varios años de encasillamiento, de Bruce Schneier, que por fin parece estar recuperado.

Manual de Hack Arroba de Andres Mendez y Manuel E. Baleriola 2000 ISBN: 1138-1655 213 páginas

Para los adictos a la revista Arroba, tienen aquí una recopilación de los artículos de Hacking, que esta revista se brinda a publicar. El texto de este libro es puro y duro y muestra todas las técnicas del Hacking por medio de ordenadores. Mostrando los aspectos más reales de cada táctica o técnica, como se le quiera llamar. A lo largo de las paginas de este manual, usted conocerá la forma de Hackera páginas Web, Ordenadores remotos o conocer las diferentes herramientas que utiliza el Hacker. Para los que ansían de conocer todas las técnicas, este es su manual. Otra cosa es si es legitimo decir las cosas con tanta frialdad. Cabe anunciar, también, que Arroba tiene pensado publicar una segunda entrega de este manual.

Virus en Internet de Mikel Urizarbarrena 1999 ISBN: 37.966.1999 380 páginas

Sin lugar a dudas, el presente libro, es uno de los más completos sobre Virus informáticos. En realidad, este libro ha sido escrito por varios miembros de la conocidaempresa Panda Software. Con esta ultima frase, sobran las palabras. Sin embargo cabe recordarle, que encontrará, a lo largo de sus páginas toda la información que necesita sobre los virus informáticos, así como especies derivadas, y como no, aprenderá a utilizar el Antivirus de Panda Software. En un momento en el que Internet, cobra especial relevancia en nuestras vidas, es muy útil conocer como son, como se crean, que son y como defenderse de los Virus informáticos que día a

día nos acechan.

Hackers ***la película* David Bischoff 1996 ISBN: 84-406-6041-3 239 páginas**

Basado en la propia película y en el guión de Rafael Moreau, Hackers, es la adaptación literaria de esta impresionante película, ya de por sí, de culto. No es la primera película que aborda el tema de los Hackers, pero si la que los marca como un hito a seguir. Dade Murphy «Zero Cold» es detenido cuando es tan solo un niño. Acusado por haber provocado el crash de Wall Street con un virus informático y con el cual infectó mas de 1.500 ordenadores conectados en la Red. Años mas tarde, recién cumplido los 18, se traslada a New York, donde conoce a los que serán un grupo de Hackers de Elite. Elllos son, Phantom Phreak, Creal Killer, Lord Nikon, Joey y la sexi Kate. Si te gusto la película, este el libro.

European Scrambling Systems de John McCormac 1996 ISBN: 1-873556-22-5 Aprox 600 páginas

European Scrambling System es ante todo, un libro de sistemas de codificación en cuanto se refiere a televisión de pago. La útima versión de este libro, es la 5, ya que parece que el autor un buen día decidió hacerlo por entregas. Una critica constructiva, ya que en realidad, lo que sucedía, es que cada vez que se terminaba de escribir un libro de este tipo, los Hackers habían puesto en circulación nuevas tácticas y sistemas de pirateo de señales de televisión. Por otro orden de cosas, el libro esta muy completo. Sedescriben en el, los ataques de los Hackers a los diferentes sistemas de encriptación de audio y video. Con todo lujo de detalles, imágenes incluidas, en el libro se describen los mas conocidos Cracks en este entorno. John MacCormak es uno de los autores más veteranos y consolidado en estos temas que se desvían del Hacking por ordenadores. Denominado Black Book, este, es un gran manual para ingenieros, electrónicos y entusiastas de la televisión encriptada.

Agradecimientos

En primer lugar le debo un especial agradecimiento a todos aquellos, que con tesón y voluntad, han escrito estupendos libros y manuales que nos son de mucha

ayuda. Otros libros, que simplemente repasan la historia de los Hackers, son también una fuente de inspiración.

Todos los libros aquí expuestos son asequibles desde la pagina criptopublicaciones de Alvaro, ex-director de la revista *Iworld* y buen amigo, o al menos nos comunicamos por E-Mail y le regale uno de mis libros con la incursión de estos títulos, en cierta manera fomento y ayudo al mismo tiempo, a que se divulgue la cultura Hacker y todos, cada día un poquito mas, sepamos de que estamos hablando.

Pero el mayor de los agradecimientos es para la ReD de Internet, porque encuentras todo lo que necesitas. Existen muchos libros mas, como el diccionario del Hacker, así como versiones electrónicas de algunos de estos libros citados aquí. Pero nómbralos todos, seria una tarea ardua y no cabrían en este libro. Así que te animo a que investigues por tu cuenta, algo que forma parte del buen investigador de los temas de la nueva cibercultura.

Glosario de términos

El glosario de términos es parte fundamental en un libro como el que tiene delante, dado que se encuentra lleno de acrónimos y palabras que mas o menos nos recuerdan algo, pero no sabemos que. En el argot de la informática, y sobre todo en la nueva cibercultura, existe todo un diccionario de acrónimos y significados. En esta sección, de obligada visita, os mostrare los detalles y significado de cada acrónimo citado en el presente libro.

address (dirección) En Internet dícese de la serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: «dirección de correo electrónico» (email address); «IP» (dirección internet); y «dirección hardware» o «dirección MAC» (hardware or MAC address).

alias (alias, apodo) Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de recordar. anonymous FTP (FTP anónimo) El FTP anónimo permite a un usuario de Internet la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en numerosos servidores de información sin tener que proporcionar su nombre de usuario y una contraseña (password). Utilizando el nombre especial de usuario anonymous, o a veces ftp, el usuario de la red podrá superar los controles localesde seguridad y podrá acceder a ficheros accesibles al público situados en un sistema remoto.

Apache (Apache) Servidor HTTP de dominio público basado en el sistema operativo Linux. Apache fue desarrollado en 1995 y es actualmente uno de los servidores HTTP más utilizados en la red.

applet (aplicacioncita, aplique) Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente. application (aplicación) Un programa que lleva a cabo una función directamente para un usuario. WWW, FTP, correo electrónico y Telnet son ejemplos de aplicaciones en el ámbito de Internet.

Appz En Internet existen miles de paginas bajo este nombre. En ellas se albergan programas completos, evidentemente crackeados. Para acceder a un Appz, dichas paginas te exigen visualizar otras paginas de contenido sexual. Los Appz son a todas luces, programas ilegales que a menudo contienen Virus embebidos.

Armouring Se trata de una técnica utilizada por algunos virus informáticos, mediante la cual se impide su examen por medio de otros programas, como por ejemplo un antivirus.

authentication (autentificación) Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

AVR Los Hackers conocen por estas siglas, las tarjetas electrónicas que permiten emular el funcionamiento de una tarjeta inteligente. En USA esta tarjeta ha sido empleada para abrir los canales de DishNet y Expresvu. En España se están empleando para abrir Vía Digital. Se denominan AVR también, porque el microcontrolador que poseen estas tarjetas es una AVR de Atmel.

backbone (columna vertebral, eje central, eje troncal) Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (stub) y de tránsito (transit) conectadas al mismo eje central están interconectadas.

BackDoor Se conoce como puerta trasera que puede estar presente en cualquier tipo de Software, ya sea un sistema operativo o el software de un microcontrolador. Los Hackers por ejemplo, hacen uso de los Backdoors para leer y escribir en tarjetas inteligentes cuando se habla de televisiones de pago.

banner (anuncio, pancarta) Imagen, gráfico o texto de carácter publicitario, normalmente de pequeño tamaño, que aparece en una página web y que habitualmente enlaza con el sitio web del anunciante.

baud (baudio) Cuando se transmiten datos, un baudio es el numero de veces que cambia el «estado» del medio de transmisión en un segundo. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo, medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

bit (bit, bitio) Unidad mínima de información digital que puede ser tratada por un ordenador. Proviene de la contracción de la expresión binary digit (dígito binario).

Bomba lógica La bomba lógica es conocida también como bomba de activación programada. La bomba lógica es un tipo de Caballo de Troya que se deja olvidado en el interior de un sistema informático como un archivo mas del sistema. Después de pasado un tiempo, cuando se cumplen las condiciones de activación, la bomba lógica despierta de su largo letargo. Se sabe que las bombas lógicas fueron bautizadas así, dado que fueron desarrolladas por trabajadores informáticos que en su día fueron despedidos, pero que esperaba vengarse tarde o temprano de sus jefes. Después de pasado un tiempo la bomba lógica se activaba y dejaba sin sospecha al trabajador despedido como presunto autor del programa.

bounce (rebote) Devolución de un mensaje de correo electrónico debido a error en la entrega al destinatario.

browser (hojeador, navegador, visor, visualizador) Aplicación para visualizar documentos WWW y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet; cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

Bucaneros: Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos.

Crackeados pasan a denominarse «piratas informáticos» así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

bug (error, insecto, gazapo) Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por Grace Murray Hooper, una de las pioneras de la programación moderna, al descubrir como un insecto (bug) había dañado un circuito del ordenador Mark. Bug 34/32 Los Hackers llaman asi, a un fallo que las tarjetas de SecaMediaguard poseen. Esto les permite Crackear dicha tarjeta.

Business Software Alliance -- BSA (Alianza del Sector del Software) Organismo creado en 1988 por diversas empresas del sector del software para defender sus derechos de propiedad intelectual sobre los programas que desarrollan. byte (byte, octeto) Conjunto significativo de ocho bits que representan un carácter. Bloquer Se trata de un artilugio que permite «bloquear» como su nombre indica, distintos comandos EMM de un canal de pago. Asi, los Hackers pueden proteger unatarjeta de acceso inteligente, frente a los cambios del contenido de dicha tarjeta por parte de la plataforma digital.

Caballo de Troya También denominados Troyanos, se trata de programas de comportamiento similar a los virus en algunos casos, dado que los caballos de Troya están diseñados para «robar» datos importantes de una maquina remota. El caballo de Troya se oculta en nuestro sistema como una aplicación de función requerida. Por ejemplo si se desea capturar una contraseña, el caballo de Troya se comportara como la aplicación Conexión telefónica a redes, para «robarnos» la contraseña, ya que al introducir esta, se realiza una copia que será enviada mas tarde por correo electrónico al autor.

cellular phone (teléfono celular, móvil, telefónico, teléfono móvil) Teléfono portátil sin hilos conectado a una red celular y que permite al usuario su empleo en cualquier lugar cubierto por la red. Una red celular, y los teléfonos a ellos conectados, puede ser digital o analógica. Si la red es digital el teléfono puede enviar y recibir información a través de Internet. chat (conversación, charla, chateo, tertulia) Comunicación simultánea entre dos o más personas a través de Internet. Hasta hace poco tiempo sólo era posible la «conversación» escrita pero los avances tecnológicos permiten ya la conversación audio y vídeo. chip (chip) Circuito integrado en un soporte de silicio, formado por transistores y otros elementos electrónicos miniaturizados. Son uno de los elementos esenciales de un ordenador. Literalmente

«astilla» o «patata frita».

click (clic, cliqueo/cliquear, pulsación/pulsar) Acción de tocar un mando cualquiera de un ratón una vez colocado el puntero del mismo sobre una determinada área de la pantalla con el fin de dar una orden al ordenador.

client (cliente) Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un fichero a un servidor de ficheros es un cliente de este servidor.

Clipper chip Dispositivo de cifrado que el Gobierno de los EE.UU. intentó hacer obligatorio mediante ley en 1995 para poder controlar el flujo de transmisiones criptografiadas a través de redes digitales de telecomunicación.

Copyhackers: Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año mas de 25 000 millones de pesetas solo en Europa.

En el año 1994 los Copyhackers vendieron tarjetas por valor de 16 000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus-Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los «bucaneros» personajes que serán detallados mas adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello «extraen» información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

cookie (cuqui, espía, delator, fisgón, galletita, pastelito, rajón, soplón) Conjunto de carecteres que se almacenan en el disco duro o en la memoria temporal del ordenador de un usuario cuando accede a las páginas de determinados sitios web. Se utilizan para que el servidor accedido pueda conocer las preferencias del usuario. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los cuquis versus cookie.

Crackers: Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers. En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la

red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica. Mas adelante hablaremos de los Cracks más famosos y difundidos en la red.

Cryptography (Criptografía) Término formado a partir del griego kruptos, «oculto» … significa, según el diccionario académico, «Arte de escribir con clave secreta o de un modo enigmático» … Es criptográfico cualquier procedimiento que permita a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, tras haberlo descifrado.

Cryptology (Criptología) Es la parte de la Criptografía que tiene por objeto el descifrado de criptogramas cuando se ignora la clave. cyber- (ciber-) Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega «cibernao», que significa «pilotar una nave».

cybercop (ciberpolicía) Funcionario policial especializado en Internet o en utilizar la red para sus investigaciones.

Cyberculture (Cibercultura) Conjunto de valores, conocimientos, creencias y experiencias generadas por la comunidad internáutica a lo largo de la historia de la red. Al principio era una cultura elitista; más tarde, con la popularización de Internet, la cibercultura es cada vez más parecida a la «cultura» a secas, aunque conserva algunas de sus peculiaridades originales.

cybernaut (cibernauta) Persona que navega por la red.

Cyberspace (Ciberespacio) Término creado por William Gibson en su novela fantástica «Neuromancer» para describir el «mundo» de los ordenadores y la sociedad creada en torno a ellos.

cybertrash (ciberbasura) Todo tipo de información almacenada o difundida por la red que es manifiestamente molesta o peligrosa para la salud mental de los internautas. Dícese también de quienes arrojan basura la red.

cyberzapping (ciberzapeo) Acción de pasar de forma rápida y compulsiva de una página a otra dentro de un sitio web o de un sitio web a otro. Dark Avenger Seudónimo de uno de los creadores de virus más famoso de todos los tiempos.

Daemon (Daemon) Aplicación UNIX que está alerta permanentemente en un servidor Intenet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página web. «Daemon» es una palabra latina que significa «espíritu» (bueno o malo) o «demonio».

Data Encryption Standard -- DES (Estándar de Cifrado de Datos) Algoritmo de

cifrado de datos estandarizado por la administración de EE.UU. de-encryption (descifrado, deencriptación) Recuperación del contenido real de una información cifrada previamente.

Defense Advanced Research Projects Agency -- DARPA (Agencia de Proyectos de Investigación Avanzada para la Defensa) Organismo dependiente del Departamento de Defensa norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET.

dialup (conexión por línea conmutada) Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre ordenadores por línea telefónica normal. Dícese también del hecho de marcar un número de teléfono digital

signature (firma digital) Información cifrada que identifica al autor de un documento electrónico y autentifica que es quien dice ser.

download (bajar, descargar) En Internet proceso de transferir información desde un servidor de información al propio ordenador

Dropper Un Dropper es un programa que no es un virus, pero que posee la capacidad de crear virus informáticos cuando se ejecuta. El Dropper así, consigue burlar los antivirus, puesto que su código no contienen nada malicioso en un principio.

Echelon Sistema de satélites norteamericanos que permiten «espiar» al usuario de a pie. El sistema Echelon permite interceptar comunicaciones de teléfono, radio o de Internet. Los satélites de Echelon no son los únicos elementos de este sistema de espionaje, ademas de ellos, podemos encontrarnos con sistemas «caputadores» de señales de radio, Escaneres y sistemas informáticos.

encryption (cifrado, encriptación) El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Enfopol Se trata de la versión Europea de Echelon. file (archivo, fichero) Unidad significativa de información que puede ser manipulada por el sistema operativo de un ordenador. Un fichero tiene una identificación única formada por un «nombre» y un «apellido», en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de fichero. Así, en el fichero prueba.txt el apellido «txt» señala que se trata de un fichero que contiene texto plano.

File Transfer Protocol -- FTP (Protocolo de Transferencia de Ficheros) Protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de unared. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo.

finger (apuntar con el dedo, dedo) Programa que muestra información acerca de

un usuario(s) especifico(s) conectado(s) a un sistema local o remoto. Habitualmente se muestra el nombre y apellidos, hora de la ultima conexión, tiempo de conexión sin actividad, línea del terminal y situación de éste. Puede también mostrar ficheros de planificación y de proyecto del usuario.

firewall (cortafuegos) Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Free Software (Software Libre) Programas desarrollados y distribuidos según la filosofía de dar al usuario la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar dichos programa (Linux es un ejemplo de esta filosofía). El software libre no es siempre software gratuito (equivocación bsatante habitual que tiene su origen en que la palabra inglesa free significa ambas cosas).

freeware (programas de libre distribución, programas gratuitos, programas de dominio público) Programas informáticos que se distribuyen a través de la red de forma gratuita.

Funcard Se trata de una variante de tarjeta electrónica basada en un microcontrolador de Atmel. Esta tarjeta electrónica esta siendo utilizada para emular sistemas de televisión de pago como SecaMediaguard o Nagra.

gateway (pasarela) Hoy se utiliza el término router (direccionador, encaminador, enrutador) en lugar de la definición original de gateway. Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes. No debería confundirse con un convertidor de protocolos.

Global System for Mobile communication -- GSM (Sistema Global para comunicaciones Móviles) Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de operadores, Administraciones Públicas y empresas. Permite la transmisión de voz y datos.

guru (gurú) Persona a la que se considera, no siempre con razón, como el sumo manantial de sabiduría sobre un determinado tema. Nicholas Negroponte es considerado el máximo gurú en lo que se refiere a Internet y la llamada Sociedad de la Información.

GriYo: Seudónimo de unos de los escritores de virus mas conocido en nuestro país.

Hackers: El primer eslabón de una sociedad «delictiva» según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación

móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de «he estado aquí» pero no modifican ni se llevan nada del ordenador atacado.

Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso.

Este grupo es el mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Heuristica Se trata de una técnica mediante la cual se examina el código de un fichero ejecutable en busca de funciones o acciones que son generalmente asociadas con la actividad vírica. Este método, utilizado por los Antivirus, a veces hacen saltar la alarma en ficheros que no están realmente afectados.

hoax (bulo, camelo) Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

host (sistema anfitrión, sistema principal / albergar, dar albergue) Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (to host) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

Irdeto Sistema de encriptación de señales digitales, de algunas plataformas de televisión alemanas. Actualmente los Hackers han dado con el algoritmo de este sistema, consiguiendo así, emular dicho sistema.

IP address (dirección IP) Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345

Joke: Se trata de una aplicación que al principio uno cree que esta ante la infección de un malicioso virus, pero en realidad se trata de una broma pesada con final feliz.

key (clave): Código de signos convenidos para la transmisión de mensajes secretos o privados. En los sistemas de televisión de pago, las Keys, son las encargadas de desencriptar las señales de televisión.

keyword (clave de búsqueda, palabra clave) Conjunto de caracteres que puede

utilizarse para buscar una información en un buscador o en un sitio web.

KeyGenerator Se denominan así, a los programas creados por Crackers, los cuales son capaces de generar las claves de registro de un programa Shareware. Estos generadores de registro, normalmente muestran el número de serie a introducir en la aplicación que se quiere registrar.

Cad KeyGenerator responde a un algoritmo especifico.

Lamers: Este grupo es quizás el que más número de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer

Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro ordenador, le fascinan enormemente.

Este es quizás el grupo que más peligro acontece en la red ya que ponen en practica todo el Software de Hackeo que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un «bombeador de correo electrónico» esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se mofa autodenominandose Hacker.

También emplean de forma habitual programas sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el ordenador esta apagado.

Toda una negligencia en un terreno tan delicado.

mail bombing (bombardeo postal) Envío indiscriminado y masivo de mensajes de correo electrónico. En la actualidad existe en Internet buena cantidad de aplicaciones que con solo pulsar un botón, permite hacer Mailbombing.

Malware Los Malware son todo tipo de software que implica una función maliciosa, como lo son los virus informáticos, los Caballos de Troya o las bombas lógicas, por citar algunos.

MBR: Es el sector de arranque propio de un disco duro, dentro de la cual se define la estructura del resto de la información contenida en el mismo. En este sentido, cada disco duro independientemente del numero de particiones que posea, si contiene un MBR único, aunque cada unidad cítese C: D: E: tiene su propio sector lógico de arranque.

MOSC Los Hackers denominan así, al arte de modificar una tarjeta de acceso

inteligente. El MOSC permite a los Hackers, recuperar el funcionamiento de una tarjeta de televisión de pago, que ha sido dada de baja. El MOSC también permite modificar los paquetes contratados en las plataformas digitales. Actualmente los Hackers son capaces de hacer MOSC en tarjetas del sistemas Irdeto, Nagra y SecaMediaguard

Modchip: El Modchip es un microcontrolador que instalado en una consola Playstation, permite leer sin problemas juegos piratas. Estos juegos se denominan piratas porque son copias alteradas de un juego original. El Modchip identifica el disco pirata y entrega a su salida el código de un disco original. Este código se denomina Boot de arranque del disco.

Nagravision: Sistema de encriptación empleado por la plataforma digital Via Digital. Su creador, Kudelski, es también el creador del sistema Nagra empleado por C+ terrestre. Ambos sistemas están Hackeados en la actualidad. Los Hackers han dado, recientemente, con el algoritmo de dichos sistemas, que en ambos casos es totalmente diferente. Nagra analógico emplea un método DES 3 y Nagra Digital un método RSA.

Newbie: Es un novato o más particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, si no que aprende.

NCSA: Son las siglas de unos de los organismos mas conocidos e importantes en el campo de la lucha antivirus. Estas siglas responden a la frase de National ComputerSecurity Association. La NCSA esta especializada en virus, evolución de los mismos y estudio para combatir a estos gérmenes de la era de la informática.

packet (paquete): La unidad de datos que se envía a través de una red. En Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino.

password (contraseña, palabra de paso) Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

pay-per-view (pago por pase, pago por visión) Servicio de televisión que permite al usuario ver un determinado programa (por ejemplo, un partido de fútbol, un concierto o una película) emitido en formato codificado, mediante el pago de una tarifa.

Pacht Es una aplicación bajo DOS o Windows que permite añadir un trozo de código a una aplicación Shareware. El código que se añade, permite registrar dicha aplicación saltándose las protecciones del Software.

Payload o Payload Activation date Los Payloads se conocen como funciones de activación de la carga explosiva. Los Payloads provienen o se emplean mucho en el campo militar, de hay la palabra de activar la carga explosiva. La función Payload aplicada a un virus informatico, implica que este se activara independientemente de la fecha en la que se infecto el PC. De esta forma se reconoce que una computadora puede infectarse un día distinto al de la reproducción de virus. Dicha activación puede ir en función de la fecha o por un determinado numero de ordenes o acciones del PC. Una vez alcanzado dichos parámetros de activación, el virus hace efecto en el PC.

Piccard Las piccards son tarjetas electrónicas basadas en el chip de Microchip, 16F84, con las cuales los Hackers han conseguido emular diferentes sistemas de pago por televisión. En 1994 los Hackers rompieron el sistema de Videocrypt con este tipo de tarjetas. En la actualidad, están siendo empleadas para CSD en toda Europa.

Poliformismo Se trata de la capacidad que poseen algunos tipos de virus que permiten mediante esta técnica, modificar la forma del propio virus cada vez que se reproduce. Con esta técnica se logra crear miles de versiones diferentes del mismo virus en tan solo unas horas. Esto implica, que el antivirus apenas puede detectarlo con seguridad. Para ello un virus polimórfico, cuenta con una pequeña cabecera que se modifica en cada infección. El resto del código no se altera, sino que simplemente se encripta por motivos de «ocultación». El algoritmo de encriptación varia de una infección a otra, mientras que la cabecera siempre actúa de activador del propio virus.

Phreaker: Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Pretty Good Privacy -- PGP (Privacidad Bastante Buena, Privacidad de las Buenas) Conocido programa de libre distribución, escrito por Phil Zimmermann, que impide, mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser leídos por otros. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autentificación del autor.

Retrovirus Se trata de un tipo de virus que ataca o impide la infección de los virus antivirus.

Rivest, Shamir, Adleman -- RSA (Rivest, Shamir, Adleman) Clave criptográfica de amplia utilización, patentada por los autores, que le dan nombre. set-top box (caja

de conexión, módulo de conexión) Dispositivo multifunción quepermite la recepción y distribución en el ámbito doméstico de señales procedentes de diversos tipos de redes de comunicación (radio, televisión, teléfono, cable, satélite, Internet, …).

Serialzs Los Serialzs están disponibles en paginas Underground en Internet. Estas paginas contienen miles de Serialzs que no son otra cosa que números de registros de aplicaciones informáticas.

shareware (programas compartidos) Dícese de los programas informáticos que se distribuyen a prueba, con el compromiso de pagar al autor su precio, normalmente bajo, una vez probado el programa y/o pasado cierto tiempo de uso.

spam (bombardeo publicitario, buzonfia) Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir «loncha de mortadela».

Sysop (Operador del sistema) Persona responsable del funcionamiento de un sistema o de una red.

Seca Mediaguard Sistema de acceso condicional empleado por la plataforma de C+ y CSD en España y resto de Europa. En la actualidad los Hackers ya conocen la forma de descodifcar las señales encriptadas bajo este formato.

Skid Kiddies (Scripts kiddies) Personas que normalmente se pasan todo el día navegando por la ReD con la sola intención de bajarse de ella todo tipo de aplicaciones.

Después, sin detenerse a leer los manuales o ficheros Leeme, ejecutan todas las aplicaciones, mientras están conectados a Internet. Esta acción, a menudo conlleva a colapsar la ReD, ya que es posible que ejecute un programa muy dañino. Un ejemplo de lo que se pretende explicar es el reciente ataque de Negacion Dos.

Sector de arranque El sector de arranque es aquella área en los discos duros, disquetes u otros dispositivos de almacenamiento, que contienen algunas de las primeras instrucciones ejecutadas por el PC cuando este arranca.

Script Los Scripts son ficheros de comandos, que permiten agrupar ordenes que se dan a través del teclado. Los Scripts son ampliamente utilizados en Internet y en programación automatizada de tareas.

Sniffers Llaman así, a las aplicaciones capaces de vigilar una conexión o sistema electrónico. También pueden recibir el nombre de caza-puertos o escaneador de puertos.

Stealth Es la técnica que permite a algunos tipos de virus permanecer ocultos en un sistema operativo y en consecuencia a cualquier aplicación Antivirus.

Tempest Los Hacerks son capaces de obtener información de un PC, aun si este no esta conectado a la ReD. La técnica denominada Tempest permite recuperar la señal RF irradiada por un monitor, para así, tener delante de sí, una copia de lo que tiene en el monitor el espiado. Los métodos Tempest son muy sofisticados y caros,

por lo que su uso esta limitado a espionajes industriales y militares.

Terminate and Stay Resident (TSR) Un TSR es un programa capaz de ejecutarse e instalar en memoria una extensión residente del mismo, la cual permanecerá activa durante todo el tiempo que el PC este activo. Después de esto, el programa finaliza su función. Los TSR no tienen porque ser especialmente dañinos, ya que por citar un ejemplo, cada vez que enciende su ordenador, este carga varios tipos de TSR, como por ejemplo el dríver del ratón.

Trigger Como su nombre indica, es un disparador, el cual permite a un programador de virus informáticos, controlar la fecha de activación del mismo.

Trojan Horse (Caballo de Troya) Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

Tunneling El Tunneling es la técnica con la cual es posible que un virus informático pueda pasar desapercibido frente a los módulos de detección, mediante punteros directos a los vectores de interrupción. Este efecto, es también empleado por los propios Antivirus actuales.

UNIX, Unix (UNIX, Unix) Sistema operativo interactivo y de tiempo compartido creado en 1969 por Ken Thompson. Reescrito a mitad de la década de los'70 por AT&T alcanzó enorme popularidad en los ambientes académicos y, más tarde en los empresariales, como un sistema portátil robusto, flexible y portable, muy utilizado en los ambientes Internet.

Underground Se conoce como Underground todo lo que esconde metodos de Hacking, Cracking o Phreaking en general. En realidad el termino Underground es empleado por los escritores para referirse a este nuevo mundo que puebla las nuevas tecnologías, y sobre todo la comunidad Internet.

virus (virus) Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

Videocrypt Sistema de encriptación de vídeo diseñado por Thomson para los canales de pago SKY en la era analógica.

Videoguard Sistema de encriptación de señales digitales de televisión, empleado actualmente por el grupo Sky.

Wildlist Bajo este nombre se esconde una lista de todos los virus conocidos. Dicha lista permite comprobar el tipo de amenazas que sufren los usuarios de computadoras.

Warez Los Warez son programas completos que se ofrecen a través de CD. Existen multitud de paginas que contienen Warez. Los Warez imcumplen los derechos de autor.

WardCard Se trata de una guerra abierta en la que intervienen únicamente tarjetas electrónicas que emulan a otras tarjetas inteligentes. En la actualidad el WardCard se basa en los ataques continuos mediante ECM, que envían las plataformas digitales como CSD o Vía, hacia las tarjetas no oficiales. Estos ataques modifican o invalidad dichas tarjetas también denominadas piratas. Después los Hackers las reactivan de nuevo. Esto es en definitiva la WardCard

wetware (materia húmeda) En la jerga de los piratas informáticos significa «cerebro».

worm (gusano) Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch &Hupp, de Xerox, en «ACM Communications» (Marzo 1982). El gusano de Internet de Noviembre de 1988 es quizás el más famoso y se propagó por si solo a más de 6.000 sistemas a lo largo de Internet.

Espero que con el contenido de este extenso Glosario, tenga a partir de ahora, las cosas un poco más claras. Todos los acrónimos aquí mencionados los habrá leído en cualquiera de las paginas de este libro. Un libro que a resumidas cuentas, contiene una gran afinidad de acrónimos y nombres que quizás nunca haya escuchado, pero que ahora ya le son conocidos. Si es usted un gran aficcionado a los temas Underground, a partir de ahora este glosario le servirá de guía.

Epilogo

Menos 4…

Karl Koch fue visto por ultima vez el 23 de mayo de 1989. Aquella mañana había acudido como de costumbre a su puesto de trabajo en una oficina de Hannover, perteneciente al partido democratacristiano alemán. Karl Koch salió de la oficina alrededor de las doce del mediodía, ante un aluvión de flashses disparados por intrépidos periodistas. Koch subió al coche y salió del aparcamiento con total naturalidad, como si aquellos periodistas, simplemente, hubieran desaparecido de repente. Tenia la intención de entregar un paquete al otro lado de la ciudad, pero dicho paquete simplemente, nunca se entrego. A media tarde sus jefes notificaron su desaparición. Y 9 días después la policía fue a un bosque de las afueras de la pequeña población de Ohof, justo en los limites de Hannover, para realizar una revisión de rutina. Alguien había denunciado que por aquella zona, había un coche abandonado el cual tenia una gruesa capa de polvo sobre la capota y el parabrisas. En la maleza, cerca del coche, la policía tropezó con un cuerpo carbonizado que yacía junto a una lata de gasolina vacía. Era Karl Koch.

Cuatro años antes, en 1985, Karl Koch había sido el primer Hacker de Alemania que había trabajado directa o indirectamente para la KGB. Desde entonces, varios han sido los Hackers que han sufrido la misma suerte, y todo por culpa del espionaje industrial. Sin embargo, no todo el espionaje obtiene los mismos resultados, es decir, es posible espiar al vecino y a lo sumo recibirás una denuncia. No obstante esto se hace muy a menudo.

Por otro orden de cosas, el espionaje se ha extendido a nuestra sociedad como un elemento mas de nuestras vida, ya sea porque necesitamos saber que hace nuestra esposa en ciertos momentos o ya sea porque nos pica el gusanillo de conocer el funcionamiento de una tarjeta inteligente. En el presente reportaje descubriremos los avatares de este tipo de espionaje. Los que, sinceramente, no surtan ningún tipo de peligro para nuestras vidas.

Menos 3…

El 24 de Octubre de 1998, un miembro de CCC «Computer Chaos Club» llamado Tron es víctima de un homicidio. Su cuerpo fue hallado en el interior del parque de Neukölln, Berlín, Alemania. Las fuentes policiales dictaminaron que había sido un suicidio, sin embargo los miembros de CCC no son de la misma opinión.

Tron fue una de las más brillantes cabezas dentro de las filas de Hackers de Europa. Tron era capaz de fabricar tarjetas prepago de teléfonos públicos, siendo así, el primero en crear las maravillosas tarjetas mágicas, lo que puso en guardia a la principal compañía de telefonía en Alemania.

Tras esta experiencia, Tron contacta con CCC y ofrece sus conocimientos técnicos, explorando todas las tecnologías, Tron inicia un largo camino en el estudio de la criptografía. Algo que le vale para entender el algoritmo de la telefonía celular y las tarjetas SIM. A partir de este momento Tron es capaz de «clonar» con éxito las tarjetas GSM, así como entender a fondo los sistemas ISDN.

Sin embargo tales conocimientos quedan al alcance de pocos, ya que Tron desaparece trágicamente. Con un carácter abierto y alegre, es difícil entender como Tron optaba por suicidarse. Dos meses después de su «muerte» la prensa informa al mundo que por fin «un ingeniero de telefonía» ha sido capaz de descifrar el contenido de cientos de cintas grabadas en el reinado de Hitler. Es acaso esto una coincidencia. Todas las sospechas están abiertas.

Menos 2…

La película Enemigo Publico de Jerry Bruckheimer «dirigida por Tony scott» narra la historia de un abogado «Will Smith» que de la noche a la mañana se ve involucrado en una desesperante persecución por parte de la CSA «algo así como la NSA actual» la cual despliega todo tipo de artilugios electrónicos de extremada tecnología, así como de un despliegue de satélites especiales, capaces de ver una hormiga en su hormiguero.

Esta película, queriendo o sin querer, nos muestra como los gobiernos «preferentemente el americano» han avanzado en este tipo de tareas. Por otro lado, la película arranca con una polémica sobre la «intimidad» de las personas, ya que estas

pueden ser espiadas en todo momento. Esta polémica causada por la «violación de la intimidad humana» es la que arranca la película hacia un despliegue de tecnologías posibles dentro de la ciencia ficción.

En estas líneas no quiero explicar la película en si, aunque si describir por lo menos de que se trata, para que con ello, el lector comprenda de que hablamos. Lo que quiero decir es que «Enemigo Publico» podría no ser una película en cuestión, si no una visión de lo que realmente existe fuera de las pantallas de cine.

Los expertos de la CSA consiguen cambiar por clones idénticos» el reloj, el bolígrafo o el pantalón de Will Smith, en la película» que no son mas que radiotransmisores de alta frecuencia. También, son capaces de interceptar todas las llamadas telefónicas que realiza nuestro abogado, pero lo más sorprendente de la película, es la visión de los satélites redirigidos desde una base de control, que permiten obtener imágenes claras de nuestro protagonista angustiado corriendo sobre los tejados de palm sprit.

En un principio esto bien podría ser el derroche de ideas de un buen guionista de Hollywod, pero Nicki y su libro nos muestra como todo esto, esta sucediendo realmente fuera de las pantallas de cine. Llegados a este punto, solo podemos optar por estudiar que pueden interceptar realmente desde Echelon o UKUSA y comprobar si realmente es tan alarmante como se plantea.

Menos 1…

En la actualidad debemos hacer referencia al denominador común investigar, ya que como se demuestra desde la prensa diaria, algo esta sucediendo en el mundo y mas concretamente en el aspecto tecnológico. La guerra de los Balcanes ha desplegado de una sola vez la más alta tecnología militar y hoy por hoy esta tecnología esta cubierta de sistemas de comunicación y ordenadores.

Esta guerra esta plagada de misterios y situaciones un tanto difíciles de controlar. Solo en la armada tiene lugar un autentico estado de investigación profunda. Los serbios emplean sistemas de cifrado para sus comunicaciones secretas, siendo estas, sumamenteútiles para la Alianza Atlantica para conocer en todo momento la posición de las posiciones Serbias.

Sin embargo, la Alianza Atlantica, lejos de poder interpretar estas

comunicaciones decide destruir todas las estaciones de comunicaciones y repetidores del país, como una clara respuesta a la incapacidad de descifrar las comunicaciones. Obligándole así, al ejercito Serbio a emplear teléfonos móviles para comunicarse. Las frecuencias radiadas por estos teléfonos, son recibidas por los aviones espías de la OTAN y transcodificadas, algo muy posible ya que el sistema GSM posee un modo de cifrado estándar.

Sin embargo la guerra no solo tiene lugar en el suelo Belgrado, en el Pentágono, la Casablanca y la propia OTAN, están siendo atacadas por Hackers Serbios a los que esporádicamente se unen sus colegas Rusos. Las intenciones, buscar pistas sobre los movimientos de la Alianza Atlantica. Pero en medio de esta guerra nace Enfopol, un sistema para «pinchar» Internet, homologo a su antecesor Echelon, Enfopol intercepta todas las tramas de Internet y bajo un sistema de inteligencia artificial, filtra la información que cree buena.

Dentro de tanta polémica se conoce la noticia de la liberación, al fin, del mayor forajido de Estados Unidos, Kevin Mitcnik uno de los Hackers más inteligentes de la actualidad. Experto en sistemas de telefonía y con gran capacidad para acceder a cualquier ordenador remoto Kevin podría jugar muy bien un papel importante en todo este conflicto.

Pero queda siempre la sospecha y no la certeza de lo dicho. Lo que sí es cierto es que todo este conflicto podría desatar una guerra dentro y fuera del terreno. La red esta siendo invadida por nuevas formas de vida más inteligentes, estamos hablando de nuevos virus mas avanzados que los polimorficos. Virus encriptados y mensajes que se multiplican en la red como el Melissa, creado por David L. Smith, quien le ha llevado a crear Melissa por no se sabe muy bien.

Después de todo esto, lo que sí queda claro es que al final se prevé que solo los Hackers tendrán una clara intervención en todo conflicto ya que se demuestra que todo funciona bajo el influjo de los ordenadores y la criptografía, y solo los Hackers tienen palabra para ello.

The End

Notas

[1] El nombre de BraKGroUp es ficticio por respeto a los miembros del grupo original. Actualmente el grupo se ha dispersado y la página ya no existe. No tomen represalias los que están leyendo esto, ya que no va dirigidos a ellos. Han desaparecido varias páginas y por supuesto varios grupos de estudio de las señales encriptadas, al tiempo que han nacido otros. Por esta razón es prácticamente imposible saber de quien se esta hablando, en este caso todos están mencionados y nadie señalado con el dedo.

Esta información es puramente educacional e informativa y no se pretende realizar ningún daño a los miembros que en su día existieron. Todo lo expuesto aquí es pura información.<<